STATEMENT OF JOHN MILLER
DEPUTY COMMISSIONER, INTELLIGENCE AND COUNTERTERRORISM
NEW YORK CITY POLICE DEPARTMENT

BEFORE THE NEW YORK CITY COUNCIL
COMMITTEE ON PUBLIC SAFETY
COMMITTEE ROOM, CITY HALL
DECEMBER 18, 2019

Good afternoon Chair Richards and Members of the Council. I am John Miller, Deputy Commissioner of Intelligence and Counterterrorism for the New York City Police Department (NYPD). I am joined by Assistant Deputy Commissioner for Legal Matters Oleg Chernyavsky and, on behalf of Police Commissioner Dermot Shea we appreciate the opportunity to speak with you today about the Department's use of surveillance technology and the ways we ensure that citizens' privacy rights are respected and upheld.

Although New York City enjoys the status of being the safest big city in the nation, we also remain the preeminent American target for violent terrorists, both foreign and homegrown. That is not speculation – it is the consensus of the global intelligence community. Since September 11, 2001, there have been more than thirty terrorist plots against New York City, with targets such as Times Square, the Brooklyn Bridge, John F. Kennedy Airport, the New York Stock Exchange, the subway system as well as major synagogues and other sites. In most cases, they have been thwarted by the efforts of the NYPD and the FBI-NYPD Joint Terrorist Task Force utilizing traditional law enforcement techniques, as well as cutting-edge crime fighting and counterterror technology.

Since June alone we have uncovered and stopped four plots in various stages. Last month a Brooklyn man who was radicalized on-line was arrested, he pledged allegiance to ISIS, and was active in encrypted pro-ISIS chatrooms, posting bomb making instructions and calling for attacks. In September, a Hizballah operative living in New Jersey was charged with terrorism related crimes after having conducted extensive surveillance on potential bombing targets in the city, such as the UN, the Statue of Liberty, Times Square and our airports and bridges. He specifically scouted these locations for structural weaknesses so as to inflict maximum damage and chaos. In August, a Queens man was charged with attempting to provide material support for ISIS after having planned a knife attack at the US Open in Flushing. He had gone so far as to purchase a tactical knife and a mask, as well as gear to film his attack. In June, a different Queens man was arrested after obtaining two handguns with obliterated serial numbers to carry out an attack on Times Square where he planned to target and kill civilians and police.

Tragically, in recent years four attacks have succeeded in striking our city; an explosion in Chelsea; a white supremacist who murdered an African-American man with a sword as a "practice run" to a larger plot; a terrorist who drove a truck into the West Side Highway Running Path which killed 8 people; and an ISIS-inspired suicide bomber who set off a homemade explosive device at the Port Authority Bus Terminal subway station that injured three individuals and himself.

As you can see, the level of threat against our city has not diminished. The dangerous work of our brave men and women, and that of our partners, can sometimes be read about in the papers, but oftentimes it is not. Our operations, methods and tools are sometimes spoken about in the media and depicted in movies, but often they are not. That is by design. The ability of law enforcement to legally employ tools and techniques, that are not spoken about in the public domain, and thus not known to those seeking to do us harm, is one of the few things, if not the only thing, that by and large keeps us one step ahead. Otherwise, I would be sitting here speaking about the many more successful attacks against our city, rather than attempts that were mostly foiled.

I want to be clear, while we are always ready to work with the Council and stakeholders in furtherance of greater transparency, we are here to voice our serious concerns over any blanket proposals aimed at advertising our most sensitive capabilities. This bill is a product of privacy advocates whose core mission ---and it is a noble one--- is to guard the privacy and rights of individuals, particularly from unreasonable government intrusion. PD shares this mission, but also takes its responsibility to protect the people of the city of New York from crime, violence and terrorism very seriously. We have to do both. Neither one can have priority over the other which is why we have to balance them. I believe in this democracy, we cannot fail at either one, or we fail at both.

September 11th forever changed how the NYPD views its mission and the world around us. We have worked tirelessly to keep our city safe while protecting and upholding constitutional rights and liberties. However, we will never forget the tragedy that befell our city and our nation on September 11, 2001; the threat will be there for my children and likely their children.

I believe it's important to stress that while conducting our sensitive criminal and counterterrorism investigations and deploying state-of-the-art technology, the value the NYPD places on privacy rights and other constitutional protections is paramount. Our criminal and counterterrorism investigations are treated with particular care because we recognize that they may, at times, implicate the First and Fourth Amendments. Accordingly, we abide not only by the U.S. Constitution and the laws of the state and the city, but also, in the case of counterterrorism operations, the Handschu Guidelines.

The Handschu Guidelines are a consent decree overseen by a federal court judge, and an independent civilian observer who sits on the Handschu Committee. The Handschu Guidelines give us a set of parameters to guide Intelligence Bureau investigations into cases involving terrorism or violent hate groups. It is important to note that a review, by the Independent Inspector General of the NYPD of ten years of investigations concluded that 100 percent of the cases reviewed were properly predicated under the Handshcu Guidelines. The Independent Civilian Observer, Steven Robinson, a respected attorney and retired federal judge, who has been able to sit in on detailed reviews of every investigation concluded in his last report, quote: "I have not had concerns about the NYPD's compliance with the Handschu Guidelines and have not observed any Handschu violations."

We do not investigate purely constitutionally protected activity. Likewise, we do not conduct physical surveillance unless it is part of a documented, legally approved investigation. Electronic surveillance has to be conducted in accordance with the law or approved by a judge. We welcome

the necessarily high burden the Fourth Amendment and the State Constitution places on law enforcement.

The use of cutting edge technology is a vital component of our mission to protect this city, and none of the initiatives I speak about today would be possible without the NYPD's forward-looking embrace of emerging technology.

The NYPD has been very transparent when it comes to technology. We posted the privacy policy for our Domain Awareness System which involves both NYPD security cameras as well as private security cameras and invited the public to comment. As this council is aware, we collaborated with nearly every interested stakeholder in developing our body-worn camera policy, and worked hard to come up with a public footage release policy that leans towards transparency in critical incidents such as an officer involved shooting. Both policies were publically released. The NYPD briefed this council and then the public on when, where and how we would use UAVs or "drones" before the equipment was deployed or policy was implemented, and posted this policy on our website.

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

Intro. 487 would require granular reporting on nearly every technology used by the NYPD. The Department would be required to issue an impact and use policy about these technologies which would include their descriptions and capabilities, and consequently their limitations. The bill would prohibit the use of any new technology until after an impact and use statement is posted; the public has an opportunity to comment on it, the police commissioner reviews such comments and then issues a report. The Department would also have to amend any impact and use policy when enhancements for current technologies are sought.

The Department strongly opposes this legislation as drafted.

To be clear, the bill as currently proposed would literally require the NYPD to advertise on its website the covert means and equipment used by undercover officers who risk their lives every day. I believe that this result may not have been apparent to those advocating for this bill, however, given this fact, I can't imagine that any public official would wilfully allow this to happen. No reasonable citizen will support it. We have addressed this bill with the city council on multiple occasions. Each time we have offered suggestions for a version that would have carve-outs that do not directly endanger the lives of undercover police officers and cooperating witnesses, and would not erode our collaborative efforts with our federal and private partners. Such undercover operations and partnerships have prevented many of the attacks targeting New York City.

Let me read from the bill that is being proposed:

"The term "surveillance technology" means equipment, software, or system 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."

Now picture an undercover detective in a room. In that room a group of ISIS followers are planning an attack on Times Square. Picture another undercover detective in another room: Members of a white supremacist hate group are planning an attack on a Baptist Church in Brooklyn. Now picture

a third detective in yet another room: The leaders of a violent criminal organization are plotting to murder rivals or innocent victims. These are the types of terrifying scenarios our detectives find themselves in. We have to constantly change and adapt the technology we use to be harder to detect, because this is not a game. It's real life and undercover detectives have been killed in this city when they have been discovered. Why would we ever seek to publicly advertise those devices?

It is not just terrorism. Many of the same processes and surveillance equipment is used in criminal investigations against violent gangs, drug dealing organizations and organized crime families. How do we recruit an informant in an organized crime family if he sees the equipment we ask him to wear on our website knowing that the people he is supposed to record have seen the same thing?

We could all agree that transparency is a good thing. We could all agree that we strive for it; we even try to stretch beyond our comfort zones towards greater transparency.

But we can't do *this*.

With proper exceptions for disclosures that would endanger New Yorkers, exempting the descriptions of gear that would endanger police officers or confidential informants, consistent with exemptions in similar federal laws, we could reach a reasonable plateau. We can work together as a team to do that because we serve the same public, we guard the same rights, but we must consider not just privacy, but safety for the public and police. I've been to too many police funerals. We all went to another yesterday in Jersey City where violence and hate crimes cost the lives of a brave police officer and innocent citizens.

In addition to our robust and multi-layered internal oversight mechanisms, we operate under multiple levels of judicial, legislative, public, and academic scrutiny. We look forward to continuing this dialogue in our efforts to provide New Yorkers with the highest levels of safety and security while ensuring that all of our rights are protected.

Thank you for the opportunity to speak to this critical issue and we look forward to answering any questions you may have.

Testimony of Michael Sisitzky
On Behalf of the New York Civil Liberties Union
Before the New York City Council Committee on Public Safety
In support of Intro. 487 – The Public Oversight of Surveillance Technology Act

December 18, 2019

The New York Civil Liberties Union ("NYCLU") respectfully submits the following testimony in support of Intro. 487, the Public Oversight of Surveillance Technology ("POST") Act. 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.

NYCLU
ACLU of New York

1 Whitehall Street, 3rd Fl.
New York NY 10004
nyclu.org

Donna Lieberman
Executive Director

Robin Willner
President

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 New York Police Department ("NYPD") has a long and troubling history of engaging in surveillance tactics that target political dissent, criminalize communities of color, and jeopardize all New Yorkers' privacy. The NYCLU has litigated many cases involving NYPD surveillance abuses, including *Handschu v. Special Services Division* (challenging surveillance of political activists), *Raza v. City of New York* (challenging the NYPD's Muslim Surveillance Program), and *Millions March NYC v. NYPD* (challenging the NYPD's refusal to respond to a Freedom of Information Law ["FOIL"] request seeking information about whether the NYPD is using invasive technology to infringe on the protest rights of Black Lives Matter advocates).

Too often, the only meaningful checks on the NYPD's ability to target and surveil New Yorkers have come from court rulings or settlements in cases like these, after the harm has already been inflicted. That is due to a lack of any meaningful oversight mechanisms that could identify or preempt such harms before they occur. The public deserves to be a full partner in conversations about policing. That includes the ability to engage in robust and fully-informed conversations about what technologies are being used to target communities of color and the ways in which surveillance magnifies discrimination in areas like immigration, housing, and education.

The first step to establishing such oversight and pushing back on police surveillance that targets communities of color is to pass the POST Act.

NYCLU
ACLU of New York

I. There is No Meaningful Oversight of the NYPD's Surveillance Infrastructure

The NYPD uses numerous forms of powerful, invasive, and covert surveillance technologies to police New York City streets every day. These surveillance technologies can capture vast amounts of information about the places we visit, people we communicate with, the frequency of those communications, where we are located inside our home, and our most recent social media post.

To date, most of what we know regarding the NYPD's use of surveillance technologies is based on costly FOIL litigation by the NYCLU and other organizations, investigative journalism, and inquiries by the criminal defense community. Notably, this information is not regularly reported by the NYPD, nor is it easily obtainable from other government agencies or officials.

The NYPD is able to acquire and deploy these devices in secret because, unlike police departments in San Francisco, California;[1] Seattle, Washington;[2] Oakland, California;[3] and Cambridge, Massachusetts,[4] the Police Department is not required to seek City Council approval before obtaining new surveillance technologies. The NYPD further relies on federal grants and private donations to thwart what minimal transparency is already required under procurement rules.

While, in theory, contracts for the NYPD's purchase of surveillance technologies should be available to the public via the Comptroller, the NYPD has taken advantage of loopholes by which it can simply register contracts through the Law Department without sharing the documents with the Comptroller, request that the Comptroller withhold information in confidence, or enter into nondisclosure agreements that the NYPD cites as preventing them from releasing information to the public.[5] Alternatively, the NYPD can seek to evade any public channels whatsoever for procurement and instead

---

[1] Kate Conger, Richard Fauseet & Serge F. Kovaleski, "San Francisco Bans Facial Recognition Technology," N.Y. Times, May 14, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.
[2] ACLU of Washington, "Seattle Adopts Nation's Strongest Regulations for Surveillance Technology," Aug. 8, 2017, https://www.aclu-wa.org/news/seattle-adopts-nation%E2%80%99s-strongest-regulations-surveillance-technology.
[3] ACLU of California, "Oakland Becomes Latest Municipality to Reclaim Local Control over Surveillance Technologies Used by Local Law Enforcement," May 2, 2018, https://www.aclunc.org/news/oakland-becomes-latest-municipality-reclaim-local-control-over-surveillance-technologies-used.
[4] ACLU of Massachusetts, "Cambridge Passes Law Requiring Community Control of Police Surveillance," Dec. 10, 2018, https://www.aclum.org/en/news/cambridge-passes-law-requiring-community-control-police-surveillance.
[5] Ali Winston, "NYPD Attempts to Block Surveillance Transparency Law with Misinformation," The Intercept, July 7, 2017, https://theintercept.com/2017/07/07/nypd-surveillance-post-act-lies-misinformation-transparency/.

seek funding or equipment through the New York City Police Foundation, a private entity that provides millions of dollars per year to the Department.[6] A ProPublica report noted that, while a 2013 audit found that almost half of the $6.5 million dollars that the group gave the NYPD that year went to the Department's "technology campaign," the Foundation generally "offers no specifics at all on what its grants are used for," and that the NYPD's own budget "lumps them all into a single line item labeled 'non-city funds.'"[7]

The secretive processes by which the NYPD obtains and uses these technologies runs counter to good governance principles and threatens the digital security of all New York City residents and visitors. And without a clear mandate to disclose the tools it acquires and deploys to surveil the public in the name of public safety, these secretive processes will continue.

II. NYPD Technologies and Practices that Illustrate the Need for Transparency

The full extent of the NYPD's larger surveillance infrastructure is unknown, but what we do know is startling. More than 9,000 cameras—including both public and privately-operated surveillance cameras—are integrated into the NYPD's Domain Awareness System, alongside license plate readers, gunfire locators (ShotSpotter), environmental sensors, pattern recognition algorithms, and predictive policing tools.[8] This is complemented by a myriad of opaque databases that include systems for social media monitoring, identifying supposed gang affiliation, and the collection of DNA samples. Given the NYPD's troubling history of over-policing communities of color, the addition of advanced surveillance technologies and the data they generate to the NYPD's toolkit risks amplifying and exacerbating the harms inflicted on these communities.

Three examples in particular warrant a more detailed discussion in order to illustrate how a lack of transparency has enabled the NYPD to purchase and deploy questionable surveillance technologies.

A. Cell-Site Simulators/Stingrays

Stingrays are surveillance devices that mimic cell site towers and allow the NYPD to pinpoint a person's location, and some models can collect the phone numbers that a person has been texting and calling as well as intercept the contents of communications. When Stingrays seek information for a

---

[6] Laura Nahmias, "Police Foundation Remains a Blind Spot in NYPD Contracting Process, Critics Say," Politico, July 13, 2017, https://www.politico.com/states/new-york/city-hall/story/2017/07/13/police-foundation-remains-a-blind-spot-in-nypd-contracting-process-critics-say-113361

[7] "Private Donors Supply Spy Gear to Cops," ProPublica, Oct. 13, 2014, https://www.propublica.org/article/private-donors-supply-spy-gear-to-cops

[8] E. S. Levine, Jessica Tisch, Anthony Tasso, Michael Joy, *The New York City Police Department's Domain Awareness System*, INFORMS Journal on Applied Analytics 47(1):70-84. https://doi.org/10.1287/inte.2016.0860

targeted phone in a place as densely populated as New York City, they also sweep up information from hundreds or thousands of nearby cell phones. Stingray devices can cost over $100,000 per unit, and this does not include the additional costs of the training and maintenance packages that are necessary to use the devices.

In 2015, the NYCLU sent a FOIL request to the NYPD about Stingrays. We learned that the NYPD used these devices in more than 1,000 investigations since 2008, ranging from robbery and drug cases to criminal contempt of court.[9] The NYPD has been successful in concealing their use of Stingrays because—despite the vast amounts of personal information they could sweep up and retain—they were being used without warrants and without an internal policy guiding their use.[10] Currently, all that the public knows regarding the NYPD's use of stingrays is based on the results of our FOIL request. We still do not know the full fiscal implications of the NYPD's use of Stingrays because they have failed to reveal how many they own or which models have been purchased.

B. X-ray Vans

X-ray vans are military-grade surveillance equipment that utilize x-ray radiation to see inside of cars and buildings. These devices were used to search for roadside bombs in Afghanistan, but are also used on the streets of New York City.[11] The company that manufacturers x-ray vans determined that the vans expose bystanders to a 40% larger dose of ionizing radiation than that delivered by similar airport scanners.[12] Exposure to ionizing radiation can mutate DNA and increase the risk of cancer. In fact, the European Union and United States Transportation Security Administration banned the use of this type of radiation technology in airports citing privacy and health concerns.[13]

---

[9] NYCLU, "NYPD Has Used Stingrays more than 1,000 Times since 2008," Feb. 11, 2016, https://www.nyclu.org/en/press-releases/nypd-has-used-stingrays-more-1000-times-2008.

[10] Ciara McCarthy, "NYPD Tracked Citizens' Cellphones 1,000 Times since 2008 without Warrants," The Guardian, Feb. 11, 2016, https://www.theguardian.com/us-news/2016/feb/11/new-york-city-police-tracked-cellphones-without-warrants-stingrays.

[11] Michael Grabell, "Drive-By Scanning: Officials Expand Use and Dose of Radiation for Security Screening," ProPublica, Jan. 27, 2012, https://www.propublica.org/article/drive-by-scanning-officials-expand-use-and-dose-of-radiation-for-security-s.

[12] Conor Friedersdorf, "The NYPD Is Using Mobile X-ray Vans to Spy on Unknown Targets," The Atlantic, Oct. 19, 2015, https://www.theatlantic.com/politics/archive/2015/10/the-nypd-is-using-mobile-x-rays-to-spy-on-unknown-targets/411181/.

[13] Jack Nicas, "TSA to Halt Revealing Body Scans at Airports," The Wall Street Journal, Jan. 18, 2013, https://www.wsj.com/articles/SB10001424127887323783704578250152613273568; David DiSalvo, "Europe Bans Airport Body Scanners for 'Health and Safety' Concerns," Forbes, Nov. 15, 2011,

Additionally, x-ray vans costs between $729,000 and $825,000 per unit.[14] Until ProPublica's FOIL lawsuit, which revealed some of what we know about x-ray vans, the NYPD has largely refused to disclose anything about how it uses x-ray vans on the streets of New York. The NYPD's attempt to keep these devices secret runs counter to best practices because other agencies, including the Department of Homeland Security, already revealed the same types of information sought by ProPublica in its FOIL lawsuit.[15]

C. Face Surveillance

Face surveillance is a type of biometric recognition technology that relies on the computational analysis of images of people's faces in order to identify them. The technology, which can be used in conjunction with photographs or video footage, presents a number of civil liberties concerns, especially when considering its error rate. Face surveillance technology has repeatedly been proven to perform less accurately on African Americans, women, and people under 30. A 2018 study identified error rates of up to 34.7 percent for darker skinned females in a common, commercial face classification system.[16] Earlier this year a separate study confirmed that face recognition systems perform slower and with higher error rates on people with darker skin.[17]

Subject to no meaningful oversight, the NYPD has utilized facial recognition for almost a decade.[18] Even though access to information has been sparse, the information we do have—again, the result of litigation to force disclosure—showcases a history of highly flawed, unscientific, and even unlawful usage: from the insertion of celebrity lookalikes in lieu of actual suspect photos, to photo editing that substantially alters a suspect's actual appearance,[19] to the inclusion of mugshots of juveniles and even sealed records[20] into the NYPD's facial recognition database. The flawed uses and

---

https://www.forbes.com/sites/daviddisalvo/2011/11/15/europe-bans-airport-body-scanners-over-health-and-safety-concerns/#3e50435e2b57.

[14] Friedersdorf, *supra* note 12.

[15] Michael Grabell, "Split Decision on NYPD's X-ray Vans," ProPublica, May 10, 2016, https://www.propublica.org/article/split-decision-on-nypds-x-ray-vans.

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

[17] Cynthia M. Cook et al., *Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems,* IEEE, Feb. 6, 2019 https://ieeexplore.ieee.org/document/8636231.

[18] Clare Garvie, Georgetown Law Center on Privacy & Technology, Garbage In, Garbage Out: Face Recognition on Flawed Data, (2019), https://www.flawedfacedata.com/.

[19] *Id.*

[20] Joseph Goldstein & Ali Watkins, "She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database," N.Y. Times, Aug. 1, 2019, https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html.

error rates are made worse by the fact that, although the NYPD policy purports to require additional investigative steps to confirm a possible match prior to making an arrest, the policy is silent as to what those steps should be.[21]

Given the many flaws and inaccuracies inherent with technologies like facial recognition, the real risks of misidentification cannot be overstated, especially considering the potential for lifelong consequences that can result from even a single encounter with law enforcement. At minimum, the rules governing the use of this technology, as with all tools in the NYPD's spy kit, warrant public conversation, which the POST Act would mandate.

III. The NYPD has Already (Selectively) Followed the POST Act Formula

The process envisioned by the POST Act is straightforward. Prior to utilizing any new surveillance technology, the NYPD will be required to disclose its intended use policy, describing basic information about what the technology is, what rules the Department will adhere to, how the Department will safeguard private information against misuse, and whether the information gathered on New Yorkers will be shared with other public or private entities. This last point is critical to understanding whether New York is living up to its commitment to protect our immigrant communities from having their information end up in the hands of agencies like the Immigration and Customs Enforcement.

Following this initial publication, the public will have the opportunity to offer feedback on the proposed policies before they become final. The NYPD will also be required to post and solicit feedback on use policies for surveillance technologies already in use by the Department. To provide ongoing oversight, the legislation mandates that the Inspector General for the NYPD conduct annual audits of these policies to assess whether the NYPD is adhering to its own rules.

Critically, the NYPD has already proven that it is capable of working within this type of framework – at least, when it chooses to. When the NYPD was preparing to launch a court-ordered pilot program to study the effectiveness of body-worn cameras, the Department first prepared and published its intended policy and solicited community input through an online questionnaire, which also provided space for general feedback and commentary.[22] In the report that the NYPD issued accompanying its final policy, the Department acknowledged the utility of this type of engagement,

---

[21] Garvie, *supra* note 18.

[22] NYPD, NYPD Response to Public and Officer Input on the Department's Proposed Body-Worn Camera Policy, Apr. 2017, https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/body-worn-camera-policy-response.pdf

noting that it made several changes to the proposed policy on the basis of feedback provided by the public.[23]

On a much smaller scale, the NYPD has also proactively sought feedback from outside the Department on the use of drones. In December 2018, the NYPD publicly announced that it had acquired and would deploy 14 drones for a variety of law enforcement uses.[24] Two months prior to this public announcement, however, the NYPD reached out to the NYCLU to ask for our review of their planned policy. The NYCLU raised a number of concerns related to ambiguities in the policy's language, the potential for chilling First Amendment-protected protests and demonstrations, the need for tighter limits on the retention of footage, and the need for a more comprehensive prohibition on the use of facial recognition and other types of biometric recognition in conjunction with drone footage.[25]

While this was a tightly controlled means of soliciting feedback, it nevertheless demonstrates that the NYPD is fully capable of engaging outside stakeholders. At the time, the draft policy was shared with us in confidence. To our knowledge, the NYPD did not solicit input from other community stakeholders, absent some members of the City Council. The lack of a broader public input process was criticized when the final policy was ultimately announced, with one advocate noting that the lack of community participation reflected the NYPD's "disregard[for] the perspectives of communities most impacted by police abuses."[26] At minimum, even if broader public engagement had not led to additional substantive changes in the policy, it would have been an opportunity for the NYPD to show that it is committed to a model of community policing that actually gives voice to the communities who are policed. At its core, that is what the POST Act aims to accomplish.

IV. Disclosure is Inevitable

As noted above, other municipalities have gone much further than the POST Act would in restricting the ability of local law enforcement to acquire and deploy new surveillance technologies, with many cities and counties throughout the country now mandating that police departments seek the express approval of local legislators prior to obtaining and utilizing new surveillance tools, with some places even banning government uses of certain technologies altogether. The POST Act's transparency framework is modest compared to these other efforts. The NYPD's opposition, however, has been entirely out of proportion to the modest nature of these reforms.

---

[23] *Id.*

[24] Ashley Southall & Ali Winston, "New York Police Say They Will Deploy 14 Drones," N.Y. Times, Dec. 4, 2018, https://www.nytimes.com/2018/12/04/nyregion/nypd-drones.html.

[25] Jen Chung, "NYPD Launces Drone Program, NYCLU Warns of Overreach," Gothamist, De. 5, 2018, https://gothamist.com/news/nypd-launches-drone-program-nyclu-warns-of-overreach.

[26] Southall, *supra* note 24.

Claims that basic transparency will provide a "blueprint for those seeking to do us harm"[27] are patently in bad faith and fundamentally misrepresent the information that will become public under the POST Act, which does not require the release of any operational details that could impede police investigations. Such claims also grossly overstate the degree to which surveillance technologies are actually used for counterterrorism. For instance, when the NYPD provided the NYCLU with information on the 1,106 uses of Stingrays between 2008 and May of 2015, the Department also provided a description of the top charge being investigated for each use; overwhelmingly, these devices were being used for routine criminal investigations.[28]

As more and more cities outpace New York and prove that they can make transparency work, it is also worth emphasizing that more and more information on the surveillance tools being used by law enforcement, generally, will be introduced into the public discourse. The NYPD cannot credibly claim a need to keep secret its policies governing the use of surveillance technologies that are already subject to full public disclosure in places like San Francisco, Seattle, and Nashville. More than a dozen jurisdictions have already passed surveillance transparency laws and there are more than 30 active efforts across the country to enact similar measures.[29]

To the extent that the NYPD uses a surveillance technology subject to one of these existing or forthcoming laws, information on that technology will reach the public. And to the extent that the NYPD continues to actively resist calls for transparency, civil liberties groups, public defenders, and journalists will continue to expose surveillance abuses through public records requests and in the course of criminal prosecutions. Against this backdrop, the NYPD will continue to be seen as an agency that is more committed to secrecy than it is to building trust with the communities impacted by its practices.

V. Conclusion

We thank the Committee for the opportunity to provide testimony today and for its consideration of this critically important piece of legislation. The NYCLU looks forward to working with the Council to ensure passage of the POST Act and to ensure that the communities most impacted by police surveillance have access to the basic information they need to hold law enforcement accountable.

---

[27] Winston, *supra* note 5.
[28] *See* NYPD document production in response to NYCLU FOIL request: https://www.nyclu.org/sites/default/files/releases/NYPD%20Stingray%20use.pdf.
[29] ACLU, Community Control Over Police Surveillance, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance (last accessed Dec. 17, 2019).

NEW YORK CITY COUNCIL
COMMITTEE ON PUBLIC SAFETY

HEARING:
Creating Comprehensive Reporting and
Oversight of NYPD Surveillance Technologies

DATE:
December 18, 2019

TESTIMONY OF BARRY FRIEDMAN

Jacob D. Fuchsberg Professor of Law and
Associated Professor of Politics;
Faculty Director, Policing Project
New York University School of Law

Honorable Members of the New York City Council:

You have asked me to testify about Int. No. 487-2018, a Local Law to amend the administrative code of the city of New York to create comprehensive reporting and oversight of NYPD surveillance technologies, which I will refer to simply as "the Law." I intend to speak largely in favor of the Law, because it is essential to democratic accountability. But as I explain briefly here, and elaborate below, I think as written the legislation falls short in any number of ways.

- First, although the Law properly asks the NYPD to report to the public on adoption of certain information-gathering technologies and on the policies that will govern their use, and to obtain and consider public comment, it does not require the NYPD to respond to those comments in any way. This is a form of "notice-and-comment rulemaking," but it is missing a key ingredient of such an administrative process: the requirement that the agency give reasons acknowledging why it has adopted one form of policy over another.

- Second, although I do not know, it is not entirely clear to me that the NYPD is the only agency of New York City government that acquires and uses the sort of "surveillance technology" that the Law addresses. If it is the case that more agencies use such technologies, then it is not clear to me why only the NYPD should be regulated.

- Third, I find the Law to be badly named, and in a sense that matters. Surveillance carries a negative connotation that is both under- and over- inclusive. These technologies are used in an effort to keep the people of New York City safe. Agree or disagree with them, it would be remarkable to ask the police to assure public safety and not collect any information. And indeed, although some of the technologies you seek to regulate are used for "surveillance," the deeper concern with technology of this sort is data acquisition, use, and retention. Ideally, this would be a bill about comprehensive reporting and oversight of information-gathering technologies used by any agency to prevent crime or detect wrongdoing.

- Fourth, although the Law requires a great deal of information about the use of these technologies, it is remarkably silent about *why* there is a need for regulation and what sort of impacts this body is concerned about. The use of these technologies, even for the best of motives, threatens individual privacy, First Amendment freedoms, and can—and has—led to overcriminalization and deeply troubling racial disparities, to name but a few of the central concerns. It is odd to call for disclosure about these technologies and not explain what the basis is for that disclosure.

- Fifth, I believe—and experience elsewhere has shown—that the 180 day period for evaluating existing technologies may well be too short to expect NYPD compliance.

- Finally, NYPD officials have expressed concern that revealing some of this information about the technologies it uses will permit evasion by those who would do us harm. To the extent these are arguments are offered wholesale, as a basis for absolutely no disclosure, I believe they are overstated. But, to the extent the arguments might have validity about particular technologies or particular uses, the Law makes absolutely no provision for this eventuality.

Thus, I find this Law a step in the right direction, but all things considered I would rework it somewhat before enacting it.

Background for Testimony

I am the Jacob D. Fuchsberg Professor of Law and Affiliated Professor of Politics at New York University School of Law. For over thirty years I have taught a number of courses relevant to this legislation, including Constitutional Law, Criminal Procedure, and Democratic Policing. I also am the author of numerous publications, in both the scholarly and public realm, about regulating policing, including *Unwarranted: Policing Without Permission.*

Perhaps most germane, I also am the Faculty Director of the Policing Project at NYU Law School. Our mission is to "partner with communities and police to promote public safety through transparency, equity, and democratic engagement."[1] We conduct research, but also do work on the ground all over the country, both with policing agencies and the communities they serve, to promote democratically-accountable policing. Ours is an all-stakeholders approach. Everywhere we work, we endeavor to do so both with communities affected by policing, and with the police themselves. In that way we hope to move the needle toward greater public safety that is just, non-discriminatory, and effective. We have done precisely that, here in New York. To name two examples, we joined the Open Society Foundation and the NYPD in hosting a summit on racial disparities in policing. We also worked with both the NYPD and the plaintiffs in the *Floyd* stop and frisk litigation in obtaining public input into the NYPD's policy for its use of body cameras. If you are interested in the full scope of our work, you can learn more at our website, www.policingproject.org.

The Need for "Front-End Accountability"

Legislation like this is at the core of the Policing Project's mission. To explain why that is, I would like to draw an important distinction between what we refer to as "front-end" and "back-end" accountability.

There has been a great deal of concern in this city and in the country over the last few years about the impact of policing. Some of that concern has been about the sorts of technology you seek to regulate here, for example facial recognition, license plate readers, cell site simulators, CCTV, and the like. But it also has been about uses of force and coercion, be it police shootings

[1] *Our Mission*, Policing Project, www.policingproject.org/about-landing.

or pedestrian and traffic stops. And when those issues are discussed, the word "accountability" often is used.

But there are two kinds of accountability and they are very different. Most of what we hear about is "back-end accountability." The police have done something that people feel is wrong, and they want to assign responsibility and see that there is responsive action taken. Examples include proceedings in court to exclude evidence that is obtained unlawfully, or the prosecution of officers, the creation of bodies like our Civilian Complaint Review Board, federal investigations or civil rights suits, such as around the *Floyd* litigation—which ended up with a court-appointed monitor, and the like. All these are aimed at accountability after-the-fact, after something has happened.

As I argue in my book *Unwarranted*, and in my scholarly writings, what has been almost entirely missing from policing is accountability of a very, very different sort. It is ironic, because that is the sort of accountability we find prominent in the rest of government: front-end accountability. By that I mean to say that in most of government we seek sound, public, decision-making before agencies act. Legislative bodies pass laws regulating agency conduct. Administrative agencies adopt rules and regulations. And three things are true of that sort of lawmaking: (1) the public and its representatives have a voice in what is adopted; (2) the rules themselves are transparent, which is to say we all know what they are; and (3) we do our utmost best to make sure the laws do more good than harm, that they make sense, sometimes through the use of a technique such as cost-benefit analysis.

That is exactly what most people think of when they think of democratically-accountable government. Lawmaking by public officials in a way we can all watch and comment upon, with the goal of bettering society.

Although this sort of thing is common in society, around policing not so much. We delegate power to the police in the most general of terms, asking them to assure public safety, such as in New York City Charter § 435, but give them almost no direction about how to do this.[2] The police are of course experts in public safety, just as all agencies of government are expert in their fields. All agency officials deserve a certain amount of deference and exercise a certain degree of discretion. Still, with most agencies other than the police, we do not let them just do what they choose. Rather, we always rely on this sort of front-end accountability to provide guidelines and create guardrails. We have back-end accountability throughout government too, of course: lawsuits and oversight hearings and the like. But it is unthinkable that the rest of government would run without front-end accountability.

It is worth reviewing some of the reasons that front-end accountability is essential, because these are equally true of the police as of all other agencies.

First, there is our basic commitment to democracy. In administrative government we properly rely on the expertise of the dedicated public servants who act in our name. But it is a fundamental principle of American governance that the public sets the rules and standards by which those agencies act. Governance is not supposed to happen in secret, out of view of those

[2] "The police department and force shall have the power and it shall be their duty to preserve the public peace, prevent crime, detect and arrest offenders, suppress riots, mobs and insurrections, disperse unlawful or dangerous assemblages and assemblages which obstruct the free passage of public streets, sidewalks, parks and places; protect the rights of persons and property, guard the public health, preserve order at elections and all public meetings and assemblages; subject to the provisions of law and the rules and regulations of the commissioner of traffic, regulate, direct, control and restrict the movement of vehicular and pedestrian traffic for the facilitation of traffic and the convenience of the public as well as the proper protection of human life and health; remove all nuisances in the public streets, parks and places; arrest all street mendicants and beggars; provide proper police attendance at fires; inspect and observe all places of public amusement, all places of business having excise or other licenses to carry on any business; enforce and prevent the violation of all laws and ordinances in force in the city; and for these purposes to arrest all persons guilty of violating any law or ordinance for the suppression or punishment of crimes or offenses." NEW YORK CITY CHARTER § 435(a).

who are governed. Policing is no different, though it may have special needs for secrecy in some situations, something to which I will return.

Second, that commitment to democracy assures the basic level of legitimacy that government requires in order to act effectively. Government is supposed to be a collaboration between the governed and the governors, in which public participation assures the legitimacy of the actions government takes. If anything, this is more true, not less so, around policing. We have all seen the difficulty of policing when the public resents the police and refuses to cooperate, because they question the legitimacy of what the police are doing. The Task Force on 21st Century Policing appointed by President Obama called for the "co-production" of public safety to address this issue. Three consecutive Commissioners of the NYPD—Bratton, O'Neill, and now Shea—have expressed a recognition of the importance of public support, and have embodied this notion in the form of Neighborhood Policing. What the NYPD has done in this regard can be a model for the country; indeed, we at the Policing Project are currently working with the City of Chicago, the Chicago Police Department, and grassroots activists to establish neighborhood policing in that city.

Third, we simply get better decisions when decision-making is open to many voices, even (or especially) dissenting ones. Agencies are mission-oriented, and the police are—again—no different. We want them to be that way. But mission-orientation also can lead to tunnel vision if decisions are isolated from public and critical views. People affected by policing have a lot to offer about what works and what does not, and it is essential to hear those voices and their views in order to formulate the best policy.

Two Models of Democratic Governance

I have been speaking generally about democratic governance and front-end accountability, but in this country, and this city, there are two basic models of how this operates. (There are more, but these two are both sufficient and essential to evaluate this proposed Law.)

The first model is legislative. Elected bodies pass laws that govern all of us, including those who govern in our name. That model obviously is familiar to this Council; that is your job. This model is being used around policing technologies presently. In many places in the country, municipal and state legislative bodies are adopting laws that regulate the use of specific policing technologies, such as drones or license plate readers. And in a few places in the country, legislative bodies have passed laws governing these technologies more generally. Typically those laws require policing and other government agencies to report to the city council in much the way this Law would have the NYPD report, but then leave it to the city council to approve acquisition and use of the technology. Often these laws are variations of a model statute promoted by the American Civil Liberties Union called the Community Control of Police Surveillance, or CCOPS.[3] On our website you can find a link to the CCOPS statute, as well as two variants we have drafted. One, the Authorized Police Technologies (or APT) Act, is intended to do what CCOPS does, but to make the burden of compliance somewhat more manageable.[4] The other, the Authorized Data and Police Technologies (or ADAPT) Act, adds the regulation of certain databases, such as gang

[3] *Community Control Over Police Surveillance (CCOPS) Model Bill*, ACLU, https://www.aclu.org/other/community-control-over-police-surveillance-ccops-model-bill.
[4] *Authorized Police Technologies (APT) Act Model Legislation*, Policing Project, https://www.policingproject.org/apt-act.

databases, to the mix.[5] Versions of statutes like these are in use in thirteen jurisdictions, including Seattle, Oakland, Nashville, and Cambridge, MA.[6]

The second model is administrative. Under an administrative model, legislative bodies delegate authority to administrative agencies to do the regulating. This model often is thought to be more manageable in complex and changing areas not susceptible to constant legislative monitoring, and it takes advantage of agency expertise. Legislation instructs the administrative agency in broad terms what is to happen, then the agency adopts rules and regulations, and engages in enforcement, to see that the legislative will is carried out. Agency regulation can happen in a number of ways but the most common is through notice-and-comment rulemaking. The agency proposes a rule, the public (especially affected parties) are permitted to comment, and the agency then reviews those comments and adopts a final rule. Although the agency need not adopt the public's views, the rule of law requires the agency to explain publicly the reasons it went with its final version, especially when it rejects others' views. (Often there is judicial review of this sort of process.)

The NYPD is an agency of New York City government, and it actually has experimented with forms of notice-and-comment rulemaking. I know, because the Policing Project was deeply involved with one variant, adoption of the NYPD's general order regarding body cameras. We were asked by the department to facilitate a process of public comment. Working with the court-appointed monitor in the *Floyd* case, the lawyers for the plaintiffs, and others, including members from this body, we created a survey that was made available to New Yorkers. We also created a

---

[5] *Authorized Databases and Police Technologies (ADAPT) Act Model Legislation*, Policing Project, https://www.policingproject.org/adapt-act.

[6] *See Community Control Over Police Surveillance #TakeCTRL*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance (citing "Participating Cities" graphic).

portal for more elaborate comments. We received some 30,000 surveys, and comments from about 50 organizations. We then wrote a report summarizing all of this.[7] Ultimately the NYPD considered those views, and released its own report summarizing what it had done, and why.[8]

Many advocates ultimately were unhappy with the direction the NYPD took on some issues regarding its use of body-worn cameras.[9] I was too, though I co-authored an op-ed in the *Gotham Gazette* explaining the value of the process.[10] I adhere to those views, though I think that particular process was far too exhausting to occur regularly. But the NYPD has engaged in variants, including—for example—hearing from stakeholders including Council members on its drone policy.

In some jurisdictions one variant of the administrative model is to create a police commission of lay individuals, which engages in rulemaking for the department. That is the model in Los Angeles and San Francisco. There is an advisory variant in Seattle. The Chicago City Council presently is considering an ordinance that would create such a body for that city..

The point I want to stress is that the Law you are considering is a form of administrative notice-and-comment rulemaking. In the balance of my remarks I intend to evaluate it as such.

---

[7] POLICING PROJECT, REPORT TO THE NYPD SUMMARIZING PUBLIC FEEDBACK ON ITS PROPOSED BODY-WORN CAMERA POLICY (Apr. 2017), https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/59ce7edfb0786914ba448d82/1506705121578/Report+to+the+NYPD+Summarizing+Public+Feedback+on+BWC+Policy.pdf.

[8] NYPD, NYPD RESPONSE TO PUBLIC AND OFFICER INPUT ON THE DEPARTMENT'S PROPOSED BODY-WORN CAMERA POLICY (Apr. 2017), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/body-worn-camera-policy-response.pdf.

[9] *See, e.g.*, *NYPD Body Camera Policy Ignores Community Demands for Police Accountability*, ACLU, (Apr. 7, 2017), https://www.nyclu.org/en/press-releases/nypd-body-camera-policy-ignores-community-demands-police-accountability.

[10] Barry Friedman & Maria Monomarenko, *Pulling the Public into Police Accountability*, (Apr. 13, 2017), https://www.gothamgazette.com/opinion/6869-pulling-the-public-into-police-accountability.

Why regulate police information-gathering technology?

Members of the NYPD have commented unfavorably in the past about the sort of Law you are considering.[11] Although one understandable reason is that no one likes to be told what to do, and this is an area in which the NYPD (as with other departments) long has been left to to make decisions entirely on its own, members of the NYPD have advanced a more practical reason. Public disclosure of the technology it possesses will enable those determined to do us harm to step up their game and evade detection.

I take the claim about preserving public safety very seriously. We all should. This city, like all cities, is susceptible to crime. And this city is perhaps uniquely susceptible to terrorism, as we all know too well. I live in Greenwich Village and have since 1999; the events of 9/11 are indelibly stamped in my mind.

But there are two problems with this argument advanced by the NYPD, which require that we deal with it at retail, not at wholesale. By which I mean we must address to what extent disclosure actually is a problem, and not simply use the argument as a way to avoid any and all regulation whatsoever.

First, there are all the reasons I gave above for democratic regulation of government generally. Taken to its extreme, this argument of these NYPD officials would mean there is simply no democratic oversight of how technology is deployed.

---

[11] *See, e.g.*, Alison Fox, *POST Act Would 'Help Criminals and Terrorists,' NYPD Deputy Commissioner* Says, AM NEW York, (Jun. 18, 2017), https://www.amny.com/news/post-act-would-help-criminals-and-terrorists-nypd-deputy-commissioner-says-1-13746321/; Morning Joe, *In New York City, a Battle Over a Surveillance Bill*, MSNBC, (Jun. 16, 2017), http://www.msnbc.com/morning-joe/watch/in-new-york-city-a-battle-over-a-surveillance-bill-969162307587.

Now, if the risk of harm from disclosing this information was sufficiently high, and the need for regulation very low, we might tilt in favor of allowing the NYPD simply to make its own decisions in private.

But though I cannot assess the risk fully without more information, we are all aware that the use of these technologies come replete with a series of harms. I believe that is why we are here today. These harms are not hypothetical; they are all too real. I will review a few of them briefly; I have written about them extensively elsewhere.[12]

First, the sorts of technologies we are discussing pose a very real threat to privacy. It should take no lengthy discussion to establish this. Whether it is cameras tracking our movements, or license plate readers identifying and retaining them, or facial recognition, or cell site simulators, all of these have been written about extensively in terms of their risk to individual privacy and autonomy.

Second, the availability of these technologies can chill First Amendment freedoms. This is hardly hypothetical, whether one refers to the notorious COINTELPRO efforts of law enforcement agencies during the civil rights era, or the conduct of the NYPD that led to the Handschu guidelines. There is a persistent inclination of government to investigate dissent, and it is essential to ensure that dissent is not silenced in any way.

Third, these technologies can have very serious racial impacts. Again, this is not hypothetical. We can put aside entirely if one wishes the use of any police tactic in a deliberately discriminatory way, something for which none of us including the NYPD should stand. But it simply is an unfortunate fact in our country that communities of color and immigrant communities often are poorer and plagued with more crime. Where there is crime, technology will be deployed

[12] Barry Friedman, Unwarranted: Policing Without Permission 29–233 (2017).

to attack it. The result, an unavoidable result, will be greater technological scrutiny of these communities, including, I suspect, the collection and retention of data.

Finally (though I am skipping over other harms), surveillance can lead to over-criminalization. This too is hardly hypothetical. To take just one technology, license plate readers can and are used in some places in this country to enforce traffic violations, and to track down those with outstanding warrants, warrants that too often exist because people are simply too poor to pay for their infractions. Where license plate readers are deployed, enforcement will occur. If they are deployed unevenly in a city, where they are employed most often will yield the most enforcement. In a study of Oakland, California, the Electronic Freedom Foundation established how license plate reader use was concentrated in communities of color.[13]

I want to stress that none of this means we should not use technology. There may be some technologies so dangerous we would choose to ban them entirely; I am aware, for example, that some feel that way today about facial recognition.

What it does mean, however, is that if we are to obtain the benefits of these technologies, we must ensure that we eliminate to the greatest degree possible the harms.

And the way we do that is through sound regulation. That is what the Law under consideration here aims to do.

Before moving on to whether the Law in question achieves this, I want to make one other argument in favor of regulation, one that I think is becoming clearer to policing agencies throughout the country. If we do not regulate these technologies soundly, and as the public becomes cognizant of the harms, the risk is that we simply will start to ban them. Thus, I deeply believe it is in the interests of us all, *including the police*, to support sound regulation of the sorts

[13] Dave Maass & Jeremy Gillula, *What You Can Learn from Oakland's Raw ALPR Data*, (Jan. 21, 2015), https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data.

of technologies we are discussing. The Policing Project is committed to such sound regulation, taking into account as best we are able the benefits and harms of such technologies.

Is Int. No. 487 Appropriate Regulation?

As I indicated at the outset, I believe this Law is a step in the right direction. Were it this or nothing, I'd take this. That said, I think it suffers from a number of flaws, which tilt in "both" directions, by which I mean I am going to offer some critiques I suspect those who want more regulation will find sympathetic, and some that I suspect some who want less regulation will favor. It may be that I am about to make everyone unhappy.

First, the affirmative case. The Law is a step in the right direction because it fosters the sort of transparency that is essential to democratic governance. It informs the public about the technologies the NYPD is deploying, and asks the NYPD to assess the impact of those technologies. In addition, it requires the NYPD to draft and disclose use policies. This is essential. Often the best way to maximize the benefits of a technology, while minimizing harms, is by detailing how the technology is used, including permissible and impermissible uses. This could be accomplished by legislation, but also by general orders. The Law delegates to the NYPD the responsibility of drafting use policies, and to the Inspector General of the NYPD the responsibility for auditing whether use is consistent with those policies. So far, so good.

But, as I say, there also are some serious issues with the Law, and I would like to elaborate upon them here for your consideration.

1. Why only the NYPD?

On this first point I am somewhat in ignorance, but wish to raise it anyway. Are the sorts of technologies about which you are concerned utilized only by the NYPD? If so, then this objection is irrelevant. But if not, then it stands to reason that any agency using these technologies

should be similarly regulated. For what it is worth, the ACLU's CCOPS model, as well as our related alternatives, regulate *technologies*, not agencies, and that seems the right way to go.

2. *Why "surveillance" technologies?*

The word "surveillance" is descriptive of a function these technologies can perform, and so perhaps it is apt, but it also is the case that "surveillance" often is used with negative connotations. To the extent this is so, this Law has been badly named, in an unnecessarily incendiary way, both for the public and for the NYPD.

My assumption is that this body wants the NYPD to use some of these technologies. And I assume that is because of an assessment that some of these technologies play a valuable role in fostering public safety. I also assume this body appropriates the funds for acquisition of these technologies—and I would want to go on record as saying that neither the NYPD nor any other agency ever ought to be using technologies such as those regulated by the Law that were not appropriated by a democratically-responsible body. If I am wrong about these assumptions of what the Council believes, then I do not understand why the technologies are permitted at all.

If at least some of the technologies are welcome, under some sort of regulation, and if the word "surveillance" does indeed carry a negative connotation, then I would refer to what is being regulated as "public safety" or "information-gathering" technologies.

3. *No guidance as to what impact the City Council is concerned about?*

It simply strikes me as both odd and inappropriate that this Law so clearly regulates the use of "surveillance technology" and requires the NYPD to inform us about its "impact," yet says not one word about what sorts of impacts the Council has in mind. If there were no downsides to the use of these technologies, why regulate them at all? At the least, the technologies cost money, and so if there is no benefit to them why spend the money? But as I make clear above, there are

legitimate concerns about the harms of these technologies. Given that, it behooves this body to be clearer about what precisely it wants the NYPD to evaluate. Once again, the ACLU's CCOPS model law, as well as our APT and ADAPT Acts, are quite specific in this regard and could serve as models.

4. No response to public comments by NYPD?

The keystone to the administrative model of democratic governance is rationality—agencies must adopt rules and procedures that make sense, particularly if those rules and procedures have the capacity to cause harm. As I've discussed, notifying the public, and inviting comment from those who might have relevant and useful perspectives, is important. And I would hope and assume the NYPD will take those comments seriously. Still, the Law as written is a bit of an oddity—it requires the NYPD to take comments, but gives no guidance on what the NYPD should do with them.

In the ordinary administrative model, the agency must review the comments and respond. This can be time-consuming and costly, but it serves an essential function in assuring that the agency understands what the public is saying, and based on all the relevant considerations acts in a rational and responsive way. Again, the agency need not agree with or follow those comments, but it must give a set of basic explanations for why it chose the course it did, including why it ignored public views. Those explanations are what assure the rule of law and allow public evaluation—including by this body—of what the agency is doing.

5. 180 days may be too short a time

The NYPD deploys a wide variety of technologies. Fulfilling the requirements of the Law will take time. This will be a learning experience of sorts for the NYPD. Experience in other jurisdictions suggests that more time may be needed in order to perform this task properly.

In September 2017, Seattle adopted a statute requiring use and impact statements like those proposed in the Law. That law allowed Seattle agencies two months to compile a master list of all current technologies in use, which would then need to be reviewed in the 2018-2019 year, with completed Surveillance Impact Reports (SIRs) for each technology. Although Seattle has logged twenty-nine surveillance technologies currently in use in its master list, it has only been able to complete SIRs for 15 of these technologies in the last two years.

In other jurisdictions, compliance has occurred in a boilerplate way that also is unhelpful. For example, the city of Berkeley's Police Department provided copy-and-paste paragraphs in each of its use policies regarding the civil rights and liberties impacts of data obtained from its body-worn cameras, GPS trackers, and automated license plate readers, simply stating that "these policies will ensure the data is not used in a way that would violate or infringe upon anyone/s civil rights and/or liberties. . . ."[14] This is not what the Council wants out of the NYPD, nor, I would hope, what the NYPD would aspire to do.

I would recommend the NYPD be given at least a year to come into full compliance regarding technologies already in use.

6. Provisions for legitimate concerns about security

Finally, the Law does nothing to accommodate the NYPD's security concerns regarding disclosure. As I indicated above, when confronted with legislation like this in the past, NYPD officials have expressed some concern—as noted above—about the impact on public safety of disclosure.

I lack the information to be able to assess the validity of these claims by NYPD officials. This is an argument I hear in other jurisdictions about disclosure, and certainly when it is advanced

[14] *See* City of Berkeley Police Review Commission, Regular Meeting Agenda at 21, 33, 36, (July 10, 2019).

at wholesale it is unpersuasive. It simply is not credible that revealing any use of any technology threatens public safety. And, frankly, it is the *public's* entitlement to decide what information it is safe for them to know, not any particular government official's.

But I assume the NYPD's argument is more particularized: that there are *some* things that cannot safely be revealed. Assuming there is something to the NYPD's arguments at retail, the question becomes how to assess them on a case-by-case basis. One can imagine a variety of procedures to take these concerns into account, whether it is evaluation by a small group of public officeholders such as the Public Advocate or members of this body, or judicial review.

What I do know is that if the NYPD can make the case, that is a serious matter, and a failure to address it is a shortcoming of this legislation.

Conclusion

I want to thank you for the opportunity to testify today. The matter you are considering is extremely consequential. We would of course be willing to provide any other information that could be of use.

BRENNAN CENTER FOR JUSTICE

Written Testimony of Ángel Díaz
Counsel, Liberty & National Security Program
Brennan Center for Justice *at NYU School of Law*
Before the New York City Council
Committee on Public Safety
in Support of Int. 487
December 18, 2019

Good afternoon, Chairman Richards and members of the Committee on Public Safety. My name is Ángel Díaz, and I am Counsel for the Liberty and National Security Program at the Brennan Center for Justice. I want to thank Council Members Vanessa Gibson and Brad Lander for their leadership on this issue. I'd also like to thank the 31 co-sponsors of this legislation for their support and acknowledgement of this overdue transparency measure. Finally, thank you to Chairman Richards for holding this necessary hearing and for inviting the Brennan Center to testify.

The Brennan Center is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. The Liberty and National Security Program seeks to ensure that the country's national security laws and policies remain equal to the task of protecting individual rights, constitutional values, and the rule of law. As part of that work, we actively seek greater transparency and oversight of the NYPD's surveillance tools. While emerging technologies bring opportunities for officers to do their jobs more efficiently, they also raise many issues ranging from hidden biases to the potential for misuse. Without oversight, modern surveillance poses serious risks for the civil rights and civil liberties of those most often affected by policing: communities of color and immigrant communities.

We've seen this play out before. Just last month, former Mayor Bloomberg apologized for his support of the unconstitutional stop-and-frisk program, which heavily targeted black and brown young men.[1] But without oversight of the NYPD's surveillance apparatus, we are deploying a system that can result in a digital stop-and-frisk that will be difficult to detect or redress.[2] This is why we need common

---

[1] Shane Goldmacher, *Michael Bloomberg Pushed 'Stop-and-Frisk' Policing. Now He's Apologizing*, NEW YORK TIMES, November 17, 2019, https://www.nytimes.com/2019/11/17/us/politics/michael-bloomberg-speech.html.

[2] *See* Angel Diaz, *Oversight of Face Recognition Is Needed to Avoid New Era of 'Digital Stop and Frisk'*, BRENNAN CENTER FOR JUSTICE, May 31, 2019, https://www.brennancenter.org/our-work/analysis-opinion/oversight-face-recognition-needed-avoid-new-era-digital-stop-and-frisk.

sense accountability measures in place, and why the Brennan Center urgently calls for the overdue passage of the POST Act.

When the City Council first debated the POST Act in 2017, it had the opportunity to be a leader—now, it has fallen behind. Cities across the country, including San Francisco,[3] Seattle,[4] and Nashville,[5] have all passed laws to rein in unaccountable surveillance. Each of these laws goes further than would be required under the POST Act. In some jurisdictions, police must obtain City Council approval before they can acquire new surveillance tools;[6] a growing number of cities have even passed outright bans of facial recognition technology.[7] Meanwhile, when this Council asked the Department of Information Technology and Telecommunications whether the NYPD uses facial recognition, the DoITT's representative said they did not know.[8]

The POST Act balances the need for democratic oversight and transparency with the NYPD's need to keep certain operational tactics confidential. A strong local democracy like New York City requires at least a basic level of information about what its local police are doing and how they're doing it. The POST Act asks the NYPD to provide public answers to simple questions: what information is the department collecting, with whom is the department sharing it, and what policies are in place to respect the civil rights and civil liberties of New Yorkers? The legislation does not require the disclosure of operational details that might compromise police investigations or harm public safety.

This requirement would cover technologies such as:

- **Facial Recognition.**[9] Studies of many commercially available products have found unacceptable error rates when analyzing faces that are not white and male.[10]

---

[3] *See* SAN FRANCISCO, CAL., ORDINANCE NO. 103-19, STOP SECRET SURVEILLANCE ORDINANCE, ADMINISTRATIVE CODE - ACQUISITION OF SURVEILLANCE TECHNOLOGY (adopted May 14, 2019), available at https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A.

[4] *See* SEATTLE, WASH., ORDINANCE 125,376, MUN. CODE § 14.18.080 (Supp. 2019) (adopted Oct. 5, 2018), available at https://seattle.legistar.com/LegislationDetail.aspx?ID=3380220&GUID=95404B0E-A22D-434E-A123-B3A0448BD6FA&Options=Advanced&Search=.

[5] *See* NASHVILLE, TENN., ORDINANCE NO. BL2017-646, METRO. CODE § 13.08.08 (Supp. 2019) (adopted June 7, 2017), available at https://www.nashville.gov/mc/ordinances/term_2015_2019/bl2017_646.htm.

[6] *See, e.g.*, OAKLAND, CAL., ORDINANCE NO. 13,489, MUN. CODE ch. 9.64 (Supp. 2019) (adopted May 15, 2018), available at: http://www2.oaklandnet.com/oakca1/groups/cityadministrator/documents/standard/oak070617.pdf.

[7] *See, e.g.* Caroline Haskins, *Oakland Becomes Third U.S. City to Ban Facial Recognition*, MOTHERBOARD, July 17, 2019, available at https://www.vice.com/en_us/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz.

[8] *See* New York City Council, Transcript of the Minutes of the Committee on Housing and Buildings Jointly with the Committee on Technology and the Committee on Consumer Affairs and Business Licensing, October 7, 2019, at 31, available at https://legistar.council.nyc.gov/View.ashx?M=F&ID=7786281&GUID=CB0ABFB0-CF07-4787-9CE9-142D1E65322F.

[9] *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, CENTER ON PRIVACY & TECHNOLOGY, May 16, 2019, available at https://www.flawedfacedata.com/.

[10] *See e.g.,* Joy Buolamwini and Timnit Gerbu, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. OF MACHINE LEARNING RES. (2018), available at http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

- **Social Media Monitoring.**[11] A New York court has ordered the NYPD to release unredacted documents relating to how the Department uses Dataminr software to monitor social media.[12] This was in response to a public records request filed by Black Lives Matter activists seeking records about NYPD surveillance of their social media profiles.
- **Automatic License Plate Readers.**[13] NYPD contracts with a company called Vigilant Solutions for access to its massive database of license plate reads.[14] If the NYPD shares information captured from its own license plate readers and shares it with other customers of Vigilant Solutions, it may be unwittingly sharing information about undocumented New Yorkers with ICE.[15]

The information that would be disclosed under the POST Act is essential for effective public oversight and is also too general to be a tool for those who might wish to evade lawful police surveillance. It does not provide any information about how the NYPD uses the technology in connection with specific investigations. It does not disclose where or when it might be used or how someone might avoid it. It also does not make the tools any less effective. For example, wiretaps continue to be an important investigative tool despite widespread knowledge of their existence and a strict legal framework governing their use.

While the NYPD might enjoy a brief advantage while its tools remain secret, their existence eventually comes to light—often with a scandal attached. Even a cursory look at recent news shows why NYPD cannot be trusted to police itself:

- When a surveillance photo is too blurry or otherwise inadequate for facial recognition, the NYPD runs photos of celebrity "lookalikes" or uses photo editing software to change a person's appearance.[16]
- The NYPD secretly collects DNA samples from minors as young as 12 by offering them a soda.[17]

---

[11] *See* Jessie Gomez, *New York court rules NYPD can't use Glomar to keep surveillance records secret*, MUCKROCK, January 15, 2019, available at https://www.muckrock.com/news/archives/2019/jan/15/nypd-glomar-response/.

[12] *See Millions March NYC v. New York City Police Department*, Index No. 100690/2017, January 14, 2019, available at https://www.documentcloud.org/documents/5684800-Millions-March-Nypd.html#document/p1.

[13] *See Automatic License Plate Readers*, NYCLU, available at https://www.nyclu.org/en/automatic-license-plate-readers.

[14] *See* Anthony Romero, *Documents Uncover NYPD's Vast License Plate Reader Database*, HUFFINGTON POST, January 25, 2017, available at https://www.huffpost.com/entry/documents-uncover-nypds-v_b_9070270.

[15] *See* Russell Brandom, *Exclusive: ICE is about to start tracking license plates across the US*, VERGE, January 26, 2018, available at https://www.theverge.com/2018/1/26/16932350/ice-immigration-customs-license-plate-recognition-contract-vigilant-solutions.

[16] *See* Garvie, *Garbage In, Garbage Out*, *supra* note 9.

[17] Jan Random and Ashley Southall, *N.Y.P.D. Detectives Gave a Boy, 12, a Soda. He Landed in a DNA Database*, NEW YORK TIMES, August 15, 2019, available at https://www.nytimes.com/2019/08/15/nyregion/nypd-dna-database.html.

- As of 2018, over 98% of the entries in the NYPD's gang database were listed as either Black or Hispanic.[18]

Earlier this year, the Brennan Center published a chart that tracks each of the NYPD's known surveillance tools based on publicly available information.[19] This chart tracks many of the features included in the POST Act: it describes how each tool works, outlines concerns, and analyzes NYPD policies to the extent they exist. But this report relies on public records requests and advocacy by journalists and lawyers, a costly and slow process offering limited and delayed public access to information.

For example, the Brennan Center was party to a multi-year legal dispute with the NYPD to obtain information about the Department's use of predictive policing technologies. These systems rely on algorithms to analyze large data sets and generate statistical estimates about crime. The estimates are then used to direct police resources.

But predictive policing tools have been roundly criticized by civil rights and civil liberties advocates,[20] as they often rely on historic crime data that can be expected to both reflect and recreate decades of biased enforcement against communities of color.[21] Here in New York, historic crime data might be tainted by the Department's unconstitutional stop-and-frisk program.[22] Relying on this data to inform how police officers are deployed in the future is likely to result in the same biased policing.

These concerns motivated our decision to file a public records request seeking information about the NYPD's testing, development, and use of predictive policing. After the NYPD refused to produce documents in response to our initial public records request and a subsequent appeal, we sued. A little over a year later, we received an order from the court ordering the police department to produce many of the records we had originally requested.[23] Even then, it took almost a full year from the judge's

---

[18] Josmar Trujillo and Alex S. Vitale, *Gang Takedowns in the de Blasio Era: The Dangers of "Precision Policing,"* POLICING AND SOCIAL JUSTICE PROJECT AT BROOKLYN COLLEGE (2019), at 6, available at https://static1.squarespace.com/static/5de981188ae1bf14a94410f5/t/5df14904887d561d6cc9455e/1576093963895/2019+New+York+City+Gang+Policing+Report+-+FINAL%29.pdf.

[19] Angel Diaz, *New York City Police Department Surveillance Technology*, BRENNAN CENTER FOR JUSTICE, October 4, 2019, available at https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology.

[20] *See, e.g.*, Leadership Conference on Civil and Human Rights, et al., *Predictive Policing Today: A Shared Statement of Civil Rights Concerns* August 31, 2016, available at http://civilrightsdocs.info/pdf/FINAL_JointStatementPredictivePolicing.pdf.

[21] *See, e.g.*, Jack Smith IV, *(Exclusive) Crime-Prediction Tool PredPol Amplifies Racially Biased Policing, Study Shows*, MIC, October 9, 2016, available at https://www.mic.com/articles/156286/crime-prediction-tool-pred-pol-only-amplifies-racially-biased-policing-study-shows. *See also* Laura Nahmias and Miranda Neubauer, *NYPD Testing Crime-Forecast Software*, POLITICO, July 8, 2015, available at https://www.politico.com/states/new-york/city-hall/story/2015/07/nypd-testing-crime-forecast-software-090820 (quoting maker of predictive policing software as noting the importance of assessing "how we apply statistics and data in a way that's going to be sensitive to civil rights and surveillance and privacy concerns").

[22] *See e.g.*, Benjamin Mueller, *New York Police Dept. Agrees to Curb Stop-and-Frisk Tactics*, NEW YORK TIMES, February 2, 2017, available at https://www.nytimes.com/2017/02/02/nyregion/new-york-police-dept-stop-and-frisk.html.

[23] *See* Rachel Levinson-Waldman and Erica Posey, *Court: Public Deserves to Know How NYPD Uses Predictive Policing Software*, BRENNAN CENTER FOR JUSTICE, January 28, 2018, available at https://www.brennancenter.org/blog/court-rejects-nypd-attempts-shield-predictive-policing-disclosure.

order before the NYPD finally produced some of the information in our request. While the documents we ultimately received helped to shed light on the NYPD's predictive policing system, we still do not have a full understanding of how it works.

The goal of the POST Act is to front-load oversight. The bill allows policymakers and community members to have an informed conversation about the rules of the road *before* the NYPD deploys a new technology and before another alarming headline about police surveillance. It also encourages the NYPD to be thoughtful in how it approaches new surveillance technologies. This approach can help prevent foreseeable harms to individual rights, strengthen community trust, and avoid wasting scarce resources.

In fact, the NYPD's commitment to secrecy goes beyond even the federal government's approach. The Department of Justice[24] and the Department of Homeland Security (DHS)[25] each published policies regarding their use of Stingrays. These policies require agents to get a warrant before deploying them and documenting privacy protections. DHS also publicly described its use of backscatter x-ray systems for border security; issued Privacy Impact Assessments for its use of facial recognition[26] and license plate readers[27]; and issued guidance for state and local agencies using drones, strongly recommending transparency and public outreach.[28] If federal agencies tasked with protecting our domestic national security can provide this level of transparency, surely the NYPD should do the same.

As noted in the New York Times' endorsement of the POST Act, advances in artificial intelligence make police surveillance "the newest battleground for civil liberties."[29] Unchecked, modern surveillance tools threaten to completely redefine the right to privacy, freedom of speech, and equal protection under the law. These foundational values must be jealously guarded if New York City is to remain a strong local democracy. It is unsustainable and unacceptable for NYPD surveillance to evade

---

[24] U.S. Department of Justice, Department of Justice Policy Guidance: Use of Cell-site Simulator Technology, September 3, 2015, available at https://www.justice.gov/opa/file/767321/download.

[25] Memorandum from Alejandro N. Mayorkas to Sarah Saldana, et al., *Department Policy Regarding the Use of Cell-Site Simulator Technology*, October 19, 2015, available at https://www.dhs.gov/sites/default/files/publications/Department Policy Regarding the Use of Cell-Site Simulator Technology.pdf.

[26] U.S. Department of Homeland Security, U.S. Customs and Border Protection, *Privacy Impact Assessment for the Facial Recognition Air Entry Pilot*, DHS/CBP/PIA-025, March 11, 2015, available at https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp-1-to-1-facial-recognition-air-entry-pilot-march-11-2015.pdf.

[27] U.S. Department of Homeland Security, U.S. Immigrations and Customs Enforcement, *Privacy Impact Assessment for the Acquisition and Use of License Plate Reader Data from a Commercial Service*, DHS/ICE/PIA-039, March 19, 2015, available at https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-lpr-march2015.pdf.

[28] U.S. Department of Homeland Security, Privacy, Civil Rights & Civil Liberties Unmanned Systems Working Group, *Best Practices for Protecting Privacy, Civil Rights & Civil Liberties in Unmanned Systems Programs*, December 18, 2015, available at https://www.dhs.gov/sites/default/files/publications/UAS%20Best%20Practices.pdf.

[29] New York Times Editorial Board, *San Francisco Banned Facial Recognition. New York Isn't Even Close*, NEW YORK TIMES, May 18, 2019, available at https://www.nytimes.com/2019/05/18/opinion/nypd-post-act-surveillance.html.

accountability any longer. The Brennan Center strongly supports Int. 487 and urges the Council to pass it quickly.

Thank you again for the opportunity to testify. I am happy to answer any questions.

BRENNAN CENTER FOR JUSTICE

New York City Police Department Surveillance Technology

By Ángel Díaz PUBLISHED OCTOBER 7, 2019

In every age, police forces gain access to new tools and technologies that may advance their mission to prevent and combat crime. The deployment of new technologies requires an understanding of their impacts on the fundamental rights of the communities that police serve and the development of safeguards to prevent abuse. The New York Police Department (NYPD), however, has purchased and used new surveillance technologies while attempting to keep the public and the City Council in the dark.

This chart provides an overview of the NYPD's surveillance technology, based on publicly available information, as well as the potential impact of the use of these tools. Because the police insist on complete secrecy, however, the picture is far from complete. The NYPD should not be allowed to prevent the public and its elected representatives from learning basic information necessary on these technologies, which is critical to effective oversight and the establishment of safeguards to protect the privacy and civil liberties of New Yorkers. The POST Act, introduced by Council Member Vanessa Gibson and currently supported by 28 co-sponsors, would require NYPD to take these steps.

Facial Recognition

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
Facial recognition systems attempt to identify or verify the identity of individuals based on their face. Different systems analyze face characteristics in photos or video feeds, or through real-time surveillance.	Facial recognition raises the following concerns: **Race, Gender, and Age Bias.** Numerous studies have found that facial recognition performs poorly when analyzing the faces of women, children, and people with darker skin tones.[1] This places communities already subject to over-policing at greater risk of misidentification. **Privacy.** Facial recognition is recognized as extraordinarily intrusive, challenging reasonable expectations of privacy and lacking necessary oversight. This is why a number of groups have called for a moratorium on facial recognition. **Free Speech.** Law enforcement use of facial recognition can chill the exercise of First Amendment rights by exposing protesters to persistent surveillance and identification. **Regulation.** There have been widespread calls for its regulation[2], and some cities — such as San Francisco[3]; Oakland[4], CA; and Somerville, MA[5] — have even banned its use.	Chief of Detectives Memo #3 (2012). NYPD's Facial Identification Section (FIS) runs static photos obtained from various sources, including databases of arrest photos, juvenile arrest photos of children as young as 11, and photos connected to pistol permits, among others.[6] The system analyzes a photo against those databases and generates potential matches.[7] The system will return a list of 200+ potential matches from which an FIS investigator selects one.[8] Where the footage is blurry or otherwise unusable, the NYPD can use photo editing tools to replace facial features in a reference photo so it more closely resembles those in mugshots.[9] The NYPD has also run photos of celebrities through its facial recognition system to try to identify suspects that resemble the celebrity where the original photo returned no matches.[10] The effectiveness of these techniques is doubtful.	Garbage In, Garbage Out – Face Recognition on Flawed Data (Georgetown Law Center on Privacy & Technology) The NYPD uses altered images in its facial recognition system, new documents show (The Verge) Review on the effects of age, gender, and race demographics on automatic face recognition (The Visual Computer, Volume 34) She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database (The New York Times) Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification (Proceedings of Machine Learning Research, Volume 81) NYPD ripped for abusing facial-recognition tool (NY Daily News) Coalition Letter Calling for a Federal Moratorium on Face Recognition (ACLU) Face it: Recognition technology isn't close to ready for prime-time (NY Daily News) Face it: This is risky tech. We need to put strong controls on face-recognition technology (NY Daily News) Facial Recognition Is Accurate, if You're a White Guy (The New York Times) Interactive Facial Recognition Map (Fight for the Future)

Video Analytics

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
These systems analyze surveillance camera footage and attempt to isolate people and objects within the video feed. Video analytics use algorithms to spot particular articles of clothing and luggage. Certain versions claim they can find people in surveillance footage that match a particular hair color, facial hair, and even skin tone.	Video analytics raise the following concerns: **False Positives.** Information from video analytics can be incorrect and lead to unnecessary and potentially dangerous police encounters. **Free Speech.** Video analytics, like facial recognition, can chill First Amendment activity by exposing individuals to persistent surveillance as they move about the city. **Racial Bias**. Without adequate controls, targeting individuals based on their perceived ethnicity has the ability to exasperbate racial disparities in policing. **Privacy.** Video analytics allow for persistent surveillance as individuals move throughout the city, challenging traditional expectations of privacy.	No standalone NYPD policy is available, though video analytics may fall under the Public Security Privacy Guidelines that govern the NYPD's Domain Awareness System. These guidelines make no mention of video analytics, however, and they do not include standards governing the use or storage of analytics information. IBM developed object identification technology through a partnership with the police that gave the company access to the department's camera footage.[11] The NYPD then acquired IBM's object identification system to incorporate it into the NYPD's Domain Awareness System.[12] As of April 23, 2019, IBM stopped marketing certain versions of its Video Analytics program to additional cities.[13] It is not clear what this means for IBM's existing customers. According to the NYPD, the analytics system is intended to automatically alert NYPD officials to activities, such as "suspicious package was left" or "loitering."[14] A version of IBM's Intelligent Video Analytics 2.0, which allows users to search based on ethnicity tags, was allegedly tested but never incorporated into the NYPD's broader surveillance infrastructure.[15]	IBM Intelligent Video Analytics (IBM Vendor Material) IBM Presentation Regarding NYPD Video Analytics Development (IBM) IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color (The Intercept) The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy (ACLU)

Social Media Monitoring

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
Social media monitoring can be divided loosely into three categories: (1) Monitoring or tracking an individual, a group, or an affiliation (e.g., an online hashtag) via publicly available information; (2) Using an informant, a friend of the target, or an undercover account to obtain information from a protected or private account; or (3) Using software to monitor individuals, groups, associations, or locations. Police officers can also obtain warrants or use other legal processes to direct a social media platform to provide information, such as direct messages, metadata, and subscriber information.	Social media monitoring raises the following concerns: **False Positives.** What people say and do on social media are difficult to interpret, and connections on social media can be given undue importance or misunderstood completely. **Privacy.** Social media monitoring is intrusive, challenging individuals' reasonable expectations of privacy in online communications. **Racial Bias.** In the context of gang investigations, communities of color (especially children) are more likely to have their online activity surveilled. **Free Speech.** Surveilling social media also has the potential to chill free expression, including by causing individuals to self-censor and by monitoring lawful protest activities and other forms of protected association.	NYPD Detective Guide (2013) and Operations Order 34: Use Of Social Networks for Investigative Purposes – General Procedure, New York Police Department (2012). Policies permit officers to monitor social media for information and investigative leads. Handschu Guidelines (2017). These guidelines are the result of a settlement arising out of the NYPD's unconstitutional surveillance of protesters and religious minorities. The Handschu Guidelines allow officers to carry out general topical research, but they prohibit them from searching for individuals' names.[16] However, to develop intelligence information or to detect or prevent terrorism or other unlawful activities, the NYPD is also permitted to conduct online searches in the same manner as any member of the public, which would permit the police to access popular social media platforms.[17] Various NYPD units engage in social media monitoring, including the Intelligence, Juvenile Justice, Counterterrorism, Gang Enforcement, Internal Affairs, Executive Staff Identity Protection, and Threat Assessment divisions.[18] The full extent of social media monitoring by the NYPD is unknown, but it has been used in investigations ranging from tracking alleged gang activity[19] to surveilling Black Lives Matter protesters.[20]	Government Monitoring of Social Media: Legal and Policy Challenges (Brennan Center) NYPD monitoring of Black Lives Matter protest movements via social media (The Appeal) NYPD Social Media Monitoring Policy Allows For Use Of Aliases, Has Exceptions For Terrorist Activity (Tech Dirt) Stop and Frisk Online: Theorizing Everyday Racism in Digital Policing in the Use of Social Media for Identification of Criminal Conduct and Associations (Social Media + Society, Volume 3) The Strange Aftermath of the Largest Gang Bust in New York History (Vice) Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media (Oklahoma Law Review, Volume 71) The Wildly Unregulated Practice of Undercover Cops Friending People on Facebook (The Root) To Stem Juvenile Robberies, Police Trail Youths Before the Crime (The New York Times) Undercover cops break Facebook rules to track protesters, ensnare criminals (NBC News)

Criminal Group Database, aka the "Gang Database"

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
Gang databases contain information about individuals who police regard as confirmed or suspected gang members. The criteria for inclusion in the database are not always known, but can include poorly-defined activities such as associations with suspected gang members, various styles of dress, numerous clothing colors, and certain tattoos. In some instances, activity far removed from gang connections, such as drawing a high school mascot[21] or simply frequenting an area where gangs are known to assemble[22] has landed individuals in a gang database.	Gang databases raise the following concerns: **Racial Bias.** The vague and broad criteria for inclusion, open the door to racial bias. NYPD officials have acknowledged that as many as 95 percent of the people in its gang database are Black or Latinx.[23] **Impact on immigration status.** A gang affiliation can have negative consequences for an individual's interactions with federal immigration authorities. Immigration and Customs Enforcement (ICE) agents have been known to target individuals that have been identified as gang members in police databases.[24] The extent of information sharing between the NYPD and ICE is not properly understood. **False Positives.** Gang databases are notoriously inaccurate and over-inclusive. Individuals generally do not know if they are in the database, and there is not always a mechanism for challenging their inclusion.	There is no public NYPD policy. The information we know about the NYPD's use of the gang database comes from NYPD's testimony during city council proceedings. According to the NYPD, there are two ways individuals get added to the Gang Database: (1) Self-admission of "gang membership" to a member of the NYPD[25], being identified as a gang member by two "independent and reliable sources," or "social media posts admitting to membership in a gang." It is unclear whether NYPD requires a clear declaration of membership, or if vague associations perceived by investigating officers will do. (2) If any two of the following circumstances are true: (a) Frequent presence at a known gang location (this criteria may capture huge numbers of people who have no association besides residing in an area with active gang members); (b) Possession of "gang-related documents" (without more information, it is difficult to determine what kinds of "documents" are being referred to and whether there may be innocuous reasons to possess them); (c) Association with known gang members (it is possible to have friends and family who are gang members without joining it); (d) Social media posts with known gang members while possessing known gang paraphernalia, such as beads, flags, and bandanas (there are many reasons to pose with known gang members for social media, including for safety or familial ties); (e) Scars and tattoos associated with a particular gang; or (f) Frequently wearing colors and frequent use of hand signs that are associated with a particular gang. As of June 2018, the NYPD's gang database contained around 17,600 individuals, down from a high of 34,000.[26]	Groups Demand to See Criteria for NYPD Gang Database (Courthouse News Service) NYPD Gang Database Can Turn Unsuspecting New Yorkers into instant Felons (The Intercept) NYPD honcho insists gang database saves lives, but a teary City Council member said it can have devastating consequences (NY Daily News) How Gang Victims Are Labelled as Gang Suspects (The New Yorker) The Database (BRIC TV, Vimeo video) The fight against the NYPD gang database (The Policing and Social Justice Project, Youtube video) When a Facebook Like Lands You in Jail (Brennan Center) Spotlight: The Dangers of Gang Databases and Gang Policing (The Appeal)

Predictive Policing

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
There are two types of predictive policing programs: place-based and person-based. Place-based predictive policing uses algorithms to analyze data sets in order to try to predict where certain crimes are likely to occur. These estimates are used to inform where police officers are deployed. Person-based predictive policing analyzes data sets in order to generate a list of individuals an algorithm believes are likely to commit a crime.	Predictive policing raises the following concerns: **Racial Bias.** Predictive policing tools incorporate historical policing data to generate predictions. This makes it likely that these systems will recreate biased policing practices that have resulted in the over-policing of communities of color or data that has been manipulated to reflect higher or lower incidences of crimes. For example, historical NYPD arrest data may be tainted by its unconstitutional stop-and-frisk program or by data manipulation tactics such as falsifying arrest records to meet arrest quotas. **Privacy.** Predictive policing tools undermine constitutional requirements that police should target individuals based on individualized suspicion, not statistical probability.	There is no public NYPD policy, but the department has stated that its Public Security Privacy Guidelines for the Domain Awareness System govern predictive policing. These guidelines do not refer to predictive policing systems, and they describe the Domain Awareness System as a system to "monitor public areas and public activities," which does not describe predictive policing. The NYPD uses its own proprietary system that tries to locate hotspots for a particular crime based on an unknown number and type of data inputs.[27] Much of what we know about the NYPD's system comes from the Brennan Center's three-year legal fight with the NYPD over our public records request for documents about the development and use of the system. We do not have a complete picture of the system's inputs and outputs, but the NYPD says that its system "was not designed to store, maintain, or archive output predictions."[28] The failure to archive predictions frustrates the ability to study or audit the system for bias and related concerns. NYPD correspondence with potential vendors suggests an openness to using data inputs that could function as racial proxies, though it's not known if these inputs are incorporated into the NYPD's system. These include demographic data, school enrollment, educational attainment, income levels, journey to work, poverty levels, median income, and population under age 18.[29]	NYPD Predictive Policing Documents (Brennan Center) Predictive Policing Goes to Court (Brennan Center) 'Red Flags' as New Documents Point to Blind Spots of NYPD 'Predictive Policing' (The Daily Beast) Court: Public Deserves to Know How NYPD Uses Predictive Policing Software (Brennan Center) Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice (New York University Law Review Online) The New York City Police Department's Domain Awareness System (NYPD academic article)

Cell Site Simulators, aka "Stingrays"

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
Cell site simulators, also known as Stingrays or IMSI catchers, are devices that trick phones within a certain radius into connecting to the device rather than a cell tower, thus revealing their location to the operator of the device. Police departments use cell-site simulators to pinpoint the location of phones of targeted suspects. Cell-site simulators can also log IMSI numbers (unique identifying numbers) of all mobile devices within a given area. Additionally, while there is no evidence NYPD has used this functionality, some cell-site simulators can intercept communications that a phone is sending or receiving, and they can even change the content of those communications.[30]	Cell site simulators raise the following concerns: **Privacy.** Cell-site simulators can locate and track individuals as they move throughout public and private spaces, including when they are within a location that would require a warrant to enter. They are also indiscriminate, tricking every phone within their radius into providing identifying information. In a dense city like New York, this means numerous bystander devices will be picked up along with the targeted device. **Free Speech.** Without appropriate safeguards, cell-site simulators can be used to identify the individuals who attend protests or particular houses of worship.	There is no public NYPD policy. In 2017, a Brooklyn judge held that police use of Stingrays requires a warrant supported by probable cause.[31] Prior to this ruling, NYPD stated that its practice was to obtain a pen-register order — an order issued by a judge — so long as police can show reasonable suspicion.[32] Between 2008 and 2015, NYPD used Stingrays in over 1,000 investigations.[33] There is no publicly available information on whether the police purged extraneous data.	Cellphones, Law Enforcement, and the Right to Privacy (Brennan Center) Brooklyn Court: NYPD's Use of Cell-Phone Trackers Unconstitutional (Brennan Center) Did the Police Spy on Black Lives Matter Protesters? The Answer May Soon Come Out (The New York Times) New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says (The New York Times)

Automated License Plate Readers

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
Automated license plate readers (ALPRs) are devices that are attached to police cars or fixed on poles to capture the license plates of all cars passing by. License plate reads are also frequently run against a "hot list" of, for instance, stolen cars or AMBER Alerts. In addition to license plates, ALPRs can capture photographs of cars, along with photos of the driver and passengers. This information is uploaded to a database where it can be analyzed to study movements, associations, and relationships to crimes.	ALPRs raise the following concerns: **False Positives.** Information from ALPRs can be incorrect and lead to unnecessary and potentially dangerous police encounters. **Privacy.** ALPR data can provide a detailed account of an individual's movements. It can be used to target people who visit sensitive places, such as immigration clinics, protests, or houses of worship. **Impact on Immigration Status.** Police agencies can choose to share their ALPR information with federal immigration authorities. According to a public records request, ICE has received ALPR data from 80 different police departments, including Fairfield, CT; San Diego, CA; Orange County, Texas; and Athens-Clarke County, GA; among others.[34] It is not known whether the NYPD shares ALPR data with ICE, but the Public Security Privacy Guidelines permit the sharing of ALPR information with government entities.	Public Security Privacy Guidelines (2009). License Plate Reader Devices Operations Order (2013). The NYPD operates nearly 500 license plate readers as part of its Domain Awareness System,[35] and as of 2013, the department had a database of 16 million license plate reads.[36] The NYPD has used license plate readers to collect information about the cars parked in mosque parking lots.[37] Through its contract with the vendor Vigilant Solutions, the NYPD now has access to a database that contains over 2.2 billion license plate reads.[38] Vigilant Solutions has a national database of license plates, a national network of private ALPRs, and analytical tools that allow police to "stake out" areas, predict where certain individuals may be, and track individuals outside of New York City.[39] We do not currently know if NYPD shares the data it gets from its own ALPRs with other clients of Vigilant Solutions as well as other law enforcement or federal immigration agencies, as some cities do.	Documents Reveal ICE Using Driver Location Data From Local Police for Deportations (ACLU) Documents Uncover NYPD's Vast License Plate Reader Database (ACLU) Thousands of ICE employees can access license plate reader data, emails show (The Verge) License plate reader error leads to traffic stop at gunpoint, court case (Ars Technica) Data Driven: Explore How Cops Are Collecting and Sharing Our Travel Patterns Using Automated License Plate Readers (Electronic Frontier Foundation) Privacy advocate held at gunpoint after license plate reader database mistake, lawsuit alleges (The Verge)

Domain Awareness System

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
The Domain Awareness System (DAS) is a network of cameras, software, sensors, databases, devices, and related infrastructure that provides information and analytics to police officers for the purposes of "public safety" and to "detect, deter, and prevent potential terrorist activities."	DAS raises the following concerns: **Privacy.** DAS creates a system of persistence surveillance that covers vast swaths of New York City, which can be used to monitor the movements of New Yorkers as they move throughout the city. **False Positives.** False matches from various components, such as automatic license plate readers, can place innocent people at risk of dangerous police encounters.[40] **Data May be Shared.** The extent to which information obtained from the DAS is shared with federal agencies, such as immigration authorities, remains unknown.	The system's Public Security Privacy Guidelines (2009) specify that the purpose of the DAS is to detect and prevent terrorist attacks, but the NYPD may use these technologies for ordinary police investigations, including the detection of loiterers.[41] The guidelines fail to cover technologies, such as video analytics, that have been incorporated since they were issued. The NYPD's DAS collects and analyzes data from a variety of sources in lower and midtown Manhattan, including approximately: 9,000 CCTV cameras, some owned by the NYPD and some owned by private entities that share their feeds with police.[42] ▪ 500 license plate readers,[43] plus information obtained from contractor Vigilant Solutions.[44] ▪ Radiation and chemical sensors.[45] ▪ NYPD databases, including arrest records, criminal records, etc..[46] ▪ ShotSpotter coverage (see below for additional information).[47] ▪ 911 calls.[48]	How New York City is watching you (City & State New York) NYPD Domain Awareness System (DAS) (The Institute for Operations Research and the Management Sciences) The New York City Police Department's Domain Awareness System (NYPD article, INFORMS Journal on Applied Analytics, Volume 47)

Drones

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
Drones are remotely operated aircraft — ranging in size — that can be equipped with various cameras, sensors, and other devices. For example, they can deploy cameras capable of facial recognition, and can also contain GPS trackers and Stingray devices.	Drones raise the following concerns: **Privacy.** Without proper oversight, drones can engage in forms of surveillance that can redefine reasonable expectations of privacy. Drones can also be used to collect information about bystanders who are not connected to a law enforcement investigation. These risks are largely invisible, as drones can be difficult for ordinary persons to detect or protect against depending on their size or altitude. **Free Speech.** Without proper oversight, drones can be deployed to surveill individuals in ways that chill free expression.	Patrol Guide: Use of Unmanned Aircraft System (2018). The NYPD's policy specifies that it will not equip drones with facial recognition, but it contains a large carve-out for situations where there is a "public safety concern."[49] It is unclear if there are any restrictions on running historical drone footage through a separate facial recognition system. The policy also specifies that drone footage will only be retained for 30 days, but it contains a carve-out that allows this period to be extended for various types of legal investigations.[50] According to the NYPD, the department deploys drones for uses such as crowd control, hostage situations, and reaching remote areas. The NYPD says drones will not be used for routine police patrols, to enforce traffic laws, or for "unlawful surveillance,[51] but the NYPD has deployed drones to monitor protesters at least once during the 2019 NYC Pride March.[52]	New York's New Eyes in the Sky (Slate) New York Police Say They Will Deploy 14 Drones (The New York Times) Eyes In The Sky: The Public Has Privacy Concerns About Drones (Forbes) New NYPD Drone Policy Represents A Serious Threat to Privacy (New York Civil Liberties Union)

X-ray Vans

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
These vans use "Z backscatter" x-rays that bounce off objects, allowing the police to see into vehicles and behind walls as the van drives by.	X-ray vans raise the following concerns: **Privacy.** X-ray vans raise privacy and constitutional concerns, as they potentially allow police to examine intimate details of human bodies, private vehicles, and even inside homes. **Health.** X-ray vans raise health concerns as they may expose individuals to doses of ionizing radiation.	There is no public NYPD policy. The ways in which the NYPD uses x-ray vans and for which types of investigations remain largely unknown.[53]	Split Decision on NYPD's X-ray Vans (ProPublica) NYPD has super-secret X-ray vans (New York Post) Public Sees Through NYPD X-Ray Vans (Policing Project at NYU School of Law) The NYPD Is Using Mobile X-Ray Vans to Spy on Unknown Targets (The Atlantic)

Gunshot Detection System (ShotSpotter)

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
The privately developed ShotSpotter system uses sensors to pick up sounds that appear to be gunshots. Audio snippets are automatically sent to vendor employees who attempt to verify whether the sound represents a shooting. The vendor employee then transmits information about the potential shooting to police department clients.	Gunshot detection systems raise the following concerns: **False Positives.** This system can make mistakes and confuse ordinary background noise as gunshots. **Privacy.** Recordings of ambient noise can be misued to target voice surveillance by recording audio from selected ShotSpotter devices.	There is no standalone NYPD policy, but it may be subject to the DAS's Public Security Privacy Guidelines, since gunshot detection systems are incorporated into the NYPD's Domain Awareness System. The NYPD's ShotSpotter system uses sensors that triangulate the location of sounds that may be gunshots. If a ShotSpotter employee believes a shooting occurred, the system then sends data, including audio of the incident, to the Domain Awareness System.[54] Cameras within 500 feet are programmed to capture footage before and after the suspected gunshot.[55] Investigators at the NYPD Domain Awareness System then transmit relevant data to field officers.[56]	Here's How the NYPD's Expanding ShotSpotter System Works (DNAinfo) Privacy Audit & Assessment of ShotSpotter, Inc.'s Gunshot Detection Technology (Policing Project at NYU School of Law) The NYPD's newest technology may be recording conversations (Business Insider)

DNA Database aka the Local DNA Index System

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
DNA databases contain genetic information about individuals, which can be analyzed against a suspect's DNA for a potential match. According to media reports, the NYPD's DNA database contains as many as 82,473 genetic profiles, including samples obtained from children.[57]	DNA databases raise the following concerns: **Privacy.** Biometric samples for DNA databases can be collected without appropriate standards that respect individual privacy. Individuals are not always given a full and accurate representation of how their genetic profile will be used, and there are often no protocols for deletion. In addition, voluntary samples can be collected from children that are incapable of giving informed consent. Finally, the secret collection of "abandoned" genetic samples means that many individuals have no notice that their genetic information was collected and added to a city database. **Racial Bias.** Communities of color are likely overrepresented in DNA databases resulting from overpolicing of specific communities.	Detective Guide (2013) contains redacted instructions for collecting "abandoned" DNA samples in both "controlled" and "uncontrolled" environments. Chief of Detectives Memo #17 (2010). The memo contains instructions for how to collect "abandoned" DNA samples from objects such as water bottles, bubble gum, and apples for submission to Office of the Chief Medical Examiner (OCME) for examination. Many individuals in DNA databases have never been accused or convicted of any crime, and there are limited avenues for impacted indivudials to request deletion. There are three methods for the NYPD to obtain biometric samples for DNA analysis: ▪ **Voluntary sample.** Officers can ask individuals to provide a biometric sample for DNA analysis, but they are not necessarily required to disclose that it may be used for an unlimited number of investigations and that the sample will be retained indefinitely. They are also not required to tell individuals that they are allowed to refeuse consent. At times, police collect biometric samples from children without a lawyer, parent, or guardian present. One New York State court ruled that the NYPD violated a minor's Fourth Amendment rights against unreasonable search and seizure when they collected a genetic sample for DNA analysis where they received a written consent from the minor without the presence of his parent, guardian, or attorney.[58] ▪ **Secret collection of "abandoned" samples.** NYPD officers will obtain "abandoned" genetic samples from discarded objects, such as water bottles, chewing gum, and apples. For example, police officers bring suspects into interrogation rooms, wait for the suspect to take a drink or smoke a cigarette, and collect the sample once a suspect throws the object away.[59] ▪ **Court-ordered collection.** A court will order a suspect to provide a sample for DNA profiling where the prosecution can establish: "(1) probable cause to believe the suspect has committed the crime. (2) a 'clear indication' that relevant material evidence will be found, and (3) the method used to secure it is safe and reliable."[60]	N.Y.P.D. Detectives Gave a Boy, 12, a Soda. He Landed in a DNA Database (The New York Times) NYPD detectives demanded DNA swabs from hundreds of black and Latino men while hunting killer of Howard Beach jogger (NY Daily News) How Juveniles Get Caught Up In The NYPD's Vast DNA Dragnet (Gothamist) Legal Aid Society is Working to Protect New Yorkers From 'Genetic Stop and Frisk' (NowThis News) Push to solve gun cases fuels rapid growth of New York's DNA database (NY Daily News) New York Examines Over 800 Rape Cases for Possible Mishandling of Evidence (The New York Times) Can DNA Evidence Be Too Convincing? An Acquitted Man Thinks So (The New York Times) In New York City, Gun Cases Fuel Growing, Unregulated DNA Database (The Trace) City's DNA database swells as cops log New Yorkers' genetic material (Queens Daily Eagle) OCME Laboratory Protocols (NYC Office of Chief Medical Examiner)

Body Cameras

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
Body cameras are used to record an officer's interactions with the public and store the video for future review or use in criminal or civil proceedings. While body cameras have been promoted as a tool for police accountability, they have largely functioned as evidence-gathering devices.	Body cameras raise the following concerns: **Effectiveness.** As part of the settlement related to the NYPD's unconstitutional stop-and-frisk program, a federal judge ordered the NYPD to develop a mechanism for officers to electronically record certain police encounters.[61] However, the cameras remain under the control of police, who can decide when to activate them. Even when the cameras are rolling, police officers can add audio commentary that skews public perception of an incident (e.g. yelling "stop resisting" to a cooperating person). **Privacy.** Absent safeguards, body cameras can function as mobile surveillance devices, recording information about people and places that officers encounter while on patrol, regardless of their relationship to a suspected crime. Future iterations of body cameras may be equipped with facial recognition technology,[62] raising additional concerns about privacy, effectiveness, and racial bias.	Body Camera Patrol Guide (2018). All uniformed patrol officers in New York City are equipped with body-worn cameras.[63] In New York City, members of the public can request video under the Freedom of Information Act, but when it relates to evidence in a criminal case the video is turned over to the prosecutor's office. If a camera records an officer-involved shooting or other high-profile incident, NYPD works with "relevant authorities" to determine if video can be made public.[64]	Police Body-Worn Camera Policies Body cameras can't solve all our problems (USA Today) A Big Test of Police Body Cameras Defies Expectations (The New York Times) Body-Worn Cameras: What you need to know (NYPD) The benefits of police body cams are a myth (TechCrunch) Police Body Worn Cameras: A Policy Scorecard (The Leadership Conference & Upturn) NYPD Completes Rollout of Body-Worn Cameras to All Officers on Patrol (NYPD) The Hidden Bias of Cameras (Slate)

SkyWatch & TerraHawk Surveillance Towers

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
Surveillance towers allow officers to monitor areas from several stories above street level as well as record movements within a targeted area. Each SkyWatch tower contains flood lights, a command desk, devices to detect vehicle speeds, tinted windows, digital video recorders, and customized surveillance cameras.[65] The standard equipment placed on TerraHawk towers is unknown, but their patented technology contemplates the use of surveillance cameras along with infrared detectors, motion detectors, and a thermal imaging device.[66]	Surveillance towers raise the following concerns: **Privacy.** Surveillance towers impose a feeling of persistent monitoring, challenging reasonable expectations of privacy. Surveillance towers can also be used to collect information about bystanders who are not connected to a law enforcement investigation. **Free Speech.** Persistent monitoring from surveillance towers can chill associations among individuals.	SkyWatch Detective Guide (2013), redacted. TerraHawk Detective Guide (2013), redacted. NYPD may deploy surveillance towers in response to a rise in crime within a particular area,[67] but they have also been used to monitor protests, such as Occupy Wall Street.[68] The current number of towers deployed by NYPD is unknown. Surveillance towers are also used to collect "probative" and "potentially probative" images, according to patrol guides, but the meaning of these terms is unclear. According to media reports, TerraHawk Towers have been deployed in Staten Island, Far Rockaway, Coney Island, and Howard Beach.[69] SkyWatch have also been deployed in Harlem[70], Crown Heights[71], downtown Manhattan (Zuccotti Park)[72], Bedford-Stuyvesant Brooklyn[73], and the Lower East Side of Manhattan (Tompkins Square Park)[74].	Brooklyn Bureau: NYPD Towers May Defuse Cop, Community Friction (City Limits) NYPD Removes Controversial Surveillance Tower From Tompkins Square Park (Observer)

Endnotes

1 *See*, e.g., Joy Buolamwini and Tim Gerbu, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," available at: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; *See also* Abdurrahim, S.H., Samad, S.A. & Huddin, A.B. Vis Comput (2018) 34: 1617, available at: https://doi.org/10.1007/s00371-017-1428-z; *See also* Jacob Snow, "Amazon's Face Recognition False Matched 28 Members of Congress with Mugshots," available at: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

2 *See* Coalition letter urging federal moratorium on face recognition for law enforcement and immigration enforcement purposes, available at: https://www.aclu.org/sites/default/files/field_document/2019-06-03_coalition_letter_calling_for_federal_moratorium_on_face_recognition.pdf.

3 San Francisco "Stop Secret Surveillance" ordinance, File No. 190110, available at: https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A.

4 The final revisions to Oakland's Surveillance and Community Safety Ordinance are pending, but *see* Charlie Osborne, "Oakland follows San Francisco's lead in banning facial recognition tech," ZDNet, July 19, 2019, available at: https://www.zdnet.com/article/oakland-city-follows-san-franciscos-lead-in-banning-facial-recognition-tech/.

5 *See* City of Somerville Massachussetts Agenda Item 207566, available at: http://somervillecityma.iqm2.com/Citizens/Detail_LegiFile.aspx?Frame=&MeetingID=2941&MediaPosition=&ID=20375&CssClass=.

6 *See* NYPD correspondence with DataWorks Plus, Document 020238-020312 at page 74-75 available at: https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22.

7 NYPD, *Real Time Crime Center FIS Presentation*, available at: https://drive.google.com/open?id=18yVMSMAblqcE_nAIGf9XRI-Unik8xWOh_.

8 *See id.*

9 *See id.*

10 NYPD, Real Time Crime Center Facial Identification Section (FIS), presentation by Detective Markiewicz (Sept. 17, 2018) (notes on file with Clare Garvie at Georgetown Law Center on Privacy & Technology).

11 *See* George Joseph and Kenneth Lipp, "IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search By Skin Color," *The Intercept*, September 6, 2018, available at: https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/; *see also* IBM Presentation to NYPD "IBM SVS 4.0 Research and Development Status Update 6 for NYPD," (hereinafter "IBM Presentation") October 16, 2012, available at: https://www.documentcloud.org/documents/4452844-IBM-SVS-Analytics-4-0-Plan-Update-for-NYPD-6.html.

12 *See* Vexcel Presentation "Vexcel – NYPD: Domain Awareness System; IBM Delivery Transition Review," at slide 3, available at: https://www.documentcloud.org/documents/4452846-Vexcel-NYPD-DTR-02-04-10.html.

13 IBM, Software withdrawal: IBM Intelligent Video Analytics, April 23, 2019, available at: https://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/2/897/ENUS919-092/index.html&request_locale=en.

14 *See* Statements of NYPD Inspector Salvatore DiPace, "New York City's Hidden Surveillance Network Part 2 – by Scientific American," September 16, 2011, available at: https://www.youtube.com/watch?v=LSf4YCB3Hi0I; *see also* IBM Presentation at slide 22-50.

15 George Joseph and Kenneth Lipp, "IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search By Skin Color," *The Intercept*, September 6, 2018, available at: https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/.

16 2017 Handschu Guidelines at Section IX(B)(1), available at: https://www.aclu.org/sites/all/libraries/pdf.js/web/viewer.html?file=https%3A%2F%2Fwww.aclu.org%2Fsites%2Fdefault%2Ffiles%2Ffield_document%2Fraza_exhibit_a_to_order_approving_stipulation_of_settlement_revised_handschu_guidelines.pdf#page=1&zoom=auto,-14,800

17 *See id.* at Section IX(B)(2).

18 *See* Office of Community Oriented Policing Services, U.S. Department of Justice and Police Executive Research Forum, "Social Media and Tactical Considerations" at 13 (2013) (identifying NYPD units that engage in social media monitoring, and exploring use by Intelligence and Juvenile Justice as case studies), available at: https://www.policeforum.org/assets/docs/Free_Online_Documents/Technology/social%20media%20and%20tactical%20considerations%20for%20law%20enforcement%202013.pdf.

19 *See* David Uberti, "How Social-Media Surveillance of Teenagers Led to a New King of Policing," *The Nation*, April 19, 2019, available at: https://www.thenation.com/article/jeffery-lane-digital-street-book-review/.

20 *See id.* at 13-16; *see also* George Joseph, "Years After Protests, NYPD Retains Photos of Black Lives Matter Activists," The Appeal, January 17, 2019, available at: https://theappeal.org/years-after-protests-nypd-retains-photos-of-black-lives-matter-activists/.

21 *See* Hannah Dreier, "He Drew His School Mascot – and ICE Labeled Him a Gang Member," *ProPublica*, December 27, 2018, available at: https://features.propublica.org/ms-13-immigrant-students/huntington-school-deportations-ice-honduras/.

22 *See* Ali Winston "Vague Rules Let Ice Depoart Undocumented Immigrants as Gang Members" *The Intercept*, February 17, 2017, available at: https://theintercept.com/2017/02/17/loose-classification-rules-give-ice-broad-authority-to-classify-immigrants-as-gang-members/.

23 *See* Jeff Coltin, "Why everyone is suddenly talking about the NYPD gang database," City & State New York, June 13, 2018, available at: https://www.cityandstateny.com/articles/policy/criminal-justice/why-everyone-suddenly-talking-about-nypd-gang-database.html.

24 Emmanuel Felton, "Gang Databases Are a Life Sentence for Black and Latino Communities," *Pacific Standard*, March 15, 2018, available at: https://psmag.com/social-justice/gang-databases-life-sentence-for-black-and-latino-communities.

25 *See* Statement of Chief Dermot Shea, Chief of Detectives, New York City Police Department, Before the New York City Council Committee on Public Safety, Committee Room, City Hall, June 13, 2018, at 4.

26 *See id.*

27 *See* E.S. Levine, Jessica Tisch, Anthony Tasso, and Michael Joy, "The New York City Police Department's Domain Awareness System," Informs Journal on Applied Analytics, January 18, 2017, available at: https://pubsonline.informs.org/doi/10.1287/inte.2016.0860 (subscription required).

28 *See* Affidavit of Lesa Moore, Supreme Court of the State of New York, County of New York, Index No. 160541/2016 at Page 2, available at: https://www.brennancenter.org/sites/default/files/Lesa%20Moore%20Affidavit%20in%20Compliance%20-FINAL%20-%20%28%23%20Legal%209761080%29%20%281%29.pdf.

29 *See* Predictive Forecasting of Crime, a KEYSTATS presidenation

for the New York City Police Department, at 2-7, available at http://www.brennancenter.org/sites/default/files/Keystats%20Desired%20Data%20Elements.pdf.

30 *See* Promotional Material from GammaGroup, "3G-GSM Tactical Interception & Target Location," available at: https://info.publicintelligence.net/Gamma-GSM.pdf.

31 *See New York v. Gordon*, 58 Misc.3d 544, 550-51 (2017), available at http://www.nycourts.gov/reporter/3dseries/2017/2017_27364.htm.

32 *See id*, *see also* NYPD FOIL Response to Request #15-PL-3861 at 4, available at: https://www.nyclu.org/sites/default/files/releases/NYPD%20FOIL%20Appeal%20Response%20Stingrays.pdf.

33 *See* NYPD response to NYCLU FOIL Request, available at: https://www.nyclu.org/sites/default/files/releases/NYPD%20Stingray%20use.pdf.

34 *See* Vasudha Talla, "Documents Reveal ICE Using Driver Location Data From Local Police for Deportations", March 13, 2019, available at: https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data.

35 *See* Testimony of Deputy Commissioner of Intelligence and Counterterrorism John J. Miller, New York City Policy Department, Before the New York City Council Committees on Public Safety and Fire and Criminal Justice Services, November 12, 2014, at 4.

36 *See* Joseph Goldstein, "Weekly Police Briefing Offers Snapshot of Department and Its Leader," *The New York Times*, February 10, 2013, available at: https://www.nytimes.com/2013/02/11/nyregion/weekly-briefing-provides-lengthy-snapshot-of-kelly-and-nypd.html?_r=0.

37 *See* Adam Goldman and Matt Apuzzo, "With cameras, informants, NYPD eyed mosques," *Associated Press*, February 23, 2012, available at: https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques.

38 *See* Mariko Hirose, "Documents Uncover NYPD's Vast License Plate Reader Database," ACLU, January 25, 2016, available at: https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-reader-database.

39 *See* Agreement Between New York City Police Department and Vigilant Solutions for License Plate Recognition Data & Law Enforcement Archival & Reporting Network, dated as of April 9, 2015 at Exhibit 1 (Contractor Scope of Work), available at: https://www.nyclu.org/sites/default/files/20150409_NYCC_ALPR_foil.pdf

40 *See* Colin Lecher, "Privacy advocate held at gunpoint after license plate reader database mistake, lawsuit alleges," *The Verge*, February 21, 2019, available at: https://www.theverge.com/2019/2/21/18234785/privacy-advocate-lawsuit-california-license-plate-reader.

41 *See* NYPD Public Security Privacy Guidelines, April 2, 2009 at Pages 2-3, available at: https://www1.nyc.gov/assets/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf

42 *See* Testimony of Deputy Commissioner of Intelligence and Counterterrorism John J. Miller, New York City Policy Department, Before the New York City Council Committees on Public Safety and Fire and Criminal Justice Services, November 12, 2014, at 4.

43 *Id.*

44 *See* Agreement Between New York City Police Department and Vigilant Solutions for License Plate Recognition Data & Law Enforcement Archival & Reporting Network, dated as of April 9, 2015 at Exhibit 1 (Contractor Scope of Work), available at: https://www.nyclu.org/sites/default/files/20150409_NYCC_ALPR_foil.pdf

45 *Id.*

46 *See* Thomas H. Davenport, "How Big Data is Helping the NYPD Solve Crimes Faster," Fortune, July 17 2016, available at: http://fortune.com/2016/07/17/big-data-nypd-situational-awareness/.

47 *See id.*

48 *See id.*

49 *See* William Alden, "There's a Fight Brewing Between the NYPD and Silicon Valley's Palantir," BuzzFeed News, June 28, 2017, available at: https://www.buzzfeednews.com/article/williamalden/theres-a-fight-brewing-between-the-nypd-and-silicon-valley; *see also* NYPD Patrol Guide: Use of Department Unmanned Aircraft System (UAS), available at: https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/public-pguide2.pdf#page=687.

50 *See id.*

51 *See* Ashley Southall and Ali Winston, "New York Police Say They Will Deploy 14 Drones," *The New York Times*, December 4, 2018, available at: https://www.nytimes.com/2018/12/04/nyregion/nypd-drones.html.

52 Noah Manskar, "NYC Pride March Will Be Especially Huge for Stonewall Anniversary," *Patch*, June 25, 2019, available at: https://patch.com/new-york/new-york-city/nyc-pride-march-will-be-especially-huge-stonewall-anniversary.

53 *See In the Matter of Grabell v. New York City Police Department*, 139 A.D.3d 477, 479 (2016).

54 *See* NYPD Technology: Helping the Finest Keep NYC Safe," February 17, 2017, available at: http://nypdnews.com/2017/02/nypd-technology-helping-the-finest-keep-nyc-safe/.

55 *See* Rocco Parascandola and Oren Yaniv, "De Blasio, NYPD Unveil $1.5M ShotSpotter system, detects gunshots via sensors around city and alerts police automatically," *New York Daily News*, March 16, 2015, available at: https://www.nydailynews.com/new-york/nypd-unveils-1-5m-shotspotter-system-bronx-article-1.2151679.

56 *See* NYPD Technology: Helping the Finest Keep NYC Safe," February 17, 2017, available at: http://nypdnews.com/2017/02/nypd-technology-helping-the-finest-keep-nyc-safe/.

57 *See* Jan Ransom and Ashley Southall, "N.Y.P.D. Detectives Gave a Boy, 12, a Soda. He Landed in a DNA Database," *The New York Times*, August 15, 2019, available at: https://www.nytimes.com/2019/08/15/nyregion/nypd-dna-database.html.

58 *See People v. K.M.*, 2018 N.Y. Slip Op. 28363 at *6.

59 *See, e.g. People v. Blank*, 2018 N.Y. Slip Opp 28274.

60 *See Matter of Abe A.*, 56 N.Y.2d 288, 291 (1982).

61 *See Floyd. v. City of New York*, Case 1:08-cv-01034-AT, Document 619 "Order Regarding Documenting Police-Citizen Encounters," July 19, 2018, available at: https://www.naacpldf.org/wp-content/uploads/Order-re-lower-level-doc-pilot_0.pdf.

62 Axon, a leading manufacturer of body cameras, has said it will ban the use of facial recognition in its products because the "technology is not yet reliable enough." *See* First Report of the Axon AI & Policing Technology Ethics Board, available at: https://www.policingproject.org/axon.

63 New York City Police Department Newsroom, "NYPD Completes Rollout of Body-Worn Cameras to All Officers on Patrol," March 6, 2019, available at: https://www1.nyc.gov/site/nypd/news/pr0306/nypd-completes-rollout-body-worn-cameras-all-officers-patrol#/0.

64 *See* Body-Worn Cameras, What you need to know, available at: https://www1.nyc.gov/site/nypd/about/about-nypd/equipment-tech/body-worn-cameras.page.

65 *See* FLIR SkyWatch Options, available at: https://www.flir.com/globalassets/imported-assets/document/skywatch-options.pdf.

66 *See* TerraHawk, LLC patent for "Vehicle for deploying a mobile surveillance module," available at: https://patents.justia.com/patent/9669690.

67 *See* e.g., Jen Chung, "After Bloody Weekend, NYPD Beefs Up Patrols, SkyWatch Towers," Gothamist, June 4, 2013, available at: https://gothamist.com/2013/06/04/after_bloody_weekend_nypd_beefs_up.php.

68 *See* Tana Ganeva, "Is all that NYPD surveillance legal?" Salon, November 4, 2011, available at: https://www.salon.com/2011/11/04/is_all_that_nypd_surveillance_legal/.

69 *See* Andy Cush, "Here's the Newest Tool in the NYPD's Surveillance Arsenal," Animal New York, November 15, 2012, available at: http://animalnewyork.com/2012/heres-the-newest-tool-in-the-nyps-surveillance-arsenal/.

70 *See* "NYPD Installs 'Sky Watch' in Harlem Neighborhood," CrownHeights.info, November 23, 2006, available at: http://crownheights.info/crime/3780/nypd-installs-sky-watch-in-harlem-neighborhood/.

71 *See id.*

72 *See* Nick Turse, "What Happened When I Tried to Get Some Answers About the Creepy NYPD Watchtower Monitoring OWS," AlterNet, November 6, 2011, available at: https://www.alternet.org/2011/11/what_happened_when_i_tried_to_get_some_answers_about_the_creepy_nypd_watchtower_monitoring_ows/.

73 *See* Orsianmi Burton, "An encounter with "SkyWatch" on a block in Bedford-Stuyvesant, Brooklyn, Anthropoliteia, May 8, 2014, available at: https://anthropoliteia.net/2014/05/08/an-encounter-with-sky-watch-on-a-block-in-bedford-stuyvesant-brooklyn/.

74 *See* Catherine Rafter, "NYPD Removes Controversial Surveillance Tower from Tompkins Square Park, The Observer, July 28, 2015, available at: https://observer.com/2015/07/nypd-removes-controversial-surveillance-tower-from-tompkins-square-park/.

FOR THE RECORD

SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

@ the Urban Justice Center:
40 Rector Street, 9th Floor
New York, New York 10006
www.S.T.O.P.Spying.org | (646) 602-5600

STATEMENT OF
LIZ O'SULLIVAN
TECHNOLOGY DIRECTOR
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT, INC.

BEFORE THE
COMMITTEE ON PUBLIC SAFETY
NEW YORK CITY COUNCIL

FOR A HEARING CONCERNING,
CREATING COMPREHENSIVE REPORTING AND OVERSIGHT OF NYPD
SURVEILLANCE TECHNOLOGIES

PRESENTED
DECEMBER 18, 2019

Good Afternoon, my name is Liz O'Sullivan and I am the Technology Director for the Surveillance Technology Oversight Project ("S.T.O.P."). S.T.O.P. fights to end discriminatory surveillance and challenges both individual misconduct and broader systemic failures. I am here today in support of the Public Oversight of Surveillance Technology ("POST") Act because transparency is vital to ensure the safety and freedom of New Yorkers.

We rarely acknowledge it, but math and technology are subjective. Artificial intelligence ("A.I.") is the aggregation of many human decisions, codified into an algorithm. In civil society, we call this effect "math-washing", where A.I. systems give a dangerous illusion of objectivity. The public's misguided trust of these automated decisions creates an "automation bias", blinding us to the reality of when these systems are wrong.

Human decisions and human bias infect every automated system, including biometric surveillance tools like facial recognition. The creators of these tools inject their assumptions and misassumptions on everything from gender, to physical movements, to "normal" speech patterns. If facial recognition software is programmed to only recognize two genders, what happens when it encounters someone who is transgender or non-binary?[1] When software identifies people from their physical movements, wheelchairs users can be dehumanized and misidentified as inanimate objects.[2] A speech recognition algorithm trained on only one cadence can leave those with auditory or verbal disabilities completely unheard.[3] Simply put: Bad data gives you bad results.

Marginalized communities are disproportionately impacted by A.I. bias. Algorithms only can learn from the data they are given. When biased data shapes artificial intelligence, the bias is magnified. An alarming example of this pattern is predictive policing. New Orleans' predictive policing program secretly recorded and logged the public's movements, regardless of whether they hadn't committed a crime.[4] Then, New Orleans trained its algorithm on historical crime data that showed systemic over-policing of communities of color, so the algorithm learned to target those same communities.[5]

The first step in fighting back against algorithmic bias is disclosure. But, since police AI is often hidden from public, we have to look at other sectors to understand the impact this technology is having. Take, for example, UnitedHealth Group's algorithm prioritized care for healthy white patients over sick black patients.[6] More recently, when the Apple Card was called into question

---

[1] 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.
[2] Sheri Byrne-Haber, *Disability and AI Bias*, MEDIUM, Jul. 11, 2019, https://medium.com/@sheribyrnehaber/disability-and-ai-bias-ceed271bd533.
[3] Kate Crawford, Roel Dobbe, Theodora Dryer, Genevieve Fried, Ben Green, Elizabeth Kaziunas, Amba Kak, Varoon Mathur, Erin McElroy, Andrea Nill Sánchez, Deborah Raji, Joy Lisi Rankin, Rashida Richardson, Jason Schultz, Sarah Myers West, and Meredith Whittaker, AI Now 2019 Report, NEW YORK: AI NOW INSTITUTE, 2019, https://ainowinstitute.org/AI_Now_2019_Report.html.
[4] Anna Johansson, *5 Lessons Learned From the Predictive Policing Failure in New Orleans*, VENTUREBEAT, Mar. 19, 2018, https://venturebeat.com/2018/03/19/5-lessons-learned-from-the-predictive-policing-failure-in-new-orleans/.
[5] Jay Stanley, *New Orleans Program Offers Lessons in Pitfalls of Predictive Policing*, ACLU, Mar. 15, 2018, https://www.aclu.org/blog/privacy-technology/new-orleans-program-offers-lessons-pitfalls-predictive-policing.
[6] Robert King, *New York Insurance Regulator to Probe Optum Algorithm for Racial Bias*, FIERCEHEALTHCARE, Oct. 28, 2019, https://www.fiercehealthcare.com/payer/new-york-to-probe-algorithm-used-by-optum-for-racial-bias.

about its gender bias in determining creditworthiness, it was widely condemned algorithmic bias.[7] With growing interest in biased algorithms it's clear that we can no longer allow the NYPD to hide its AI systems and their capacity for bias.

We want to know what the city is already using, what tools are already in effect, and what technologies are next. We can't rely on the NYPD to police itself. We need transparency and public accountability to ensure we have the necessary checks and balances to keep communities safe from algorithmic bias. It is critical that we have public oversight of how our city government uses these forms of technology. Today, I urge you to pass the POST Act.

[7] Neil Vigdor, *Apple Card Investigated After Gender Discrimination Complaints*, N.Y. TIMES, Nov. 10, 2019, https://www.nytimes.com/2019/11/10/business/Apple-credit-card-investigation.html.

SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

@ the Urban Justice Center:
40 Rector Street, 9th Floor
New York, New York 10006
www.S.T.O.P.Spying.org | (646) 602-5600

STATEMENT OF
ALBERT FOX CAHN, ESQ.
EXECUTIVE DIRECTOR
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT, INC.

BEFORE THE
COMMITTEE ON PUBLIC SAFETY
NEW YORK CITY COUNCIL

FOR A HEARING CONCERNING,
CREATING COMPREHENSIVE REPORTING AND OVERSIGHT OF NYPD
SURVEILLANCE TECHNOLOGIES

PRESENTED
DECEMBER 18, 2019

Good afternoon, my name is Albert Fox Cahn, and I serve as the Executive Director for the Surveillance Technology Oversight Project ("S.T.O.P."). S.T.O.P. advocates and litigates for New Yorkers' privacy, fighting discriminatory surveillance. I speak today in support of the POST Act, which would be an important step forward in strengthening police oversight, promoting public safety, and safeguarding New Yorkers' privacy rights.

Historically, the New York City Police Department ("NYPD") deployed novel and highly invasive surveillance technologies in ways that circumvented democratic oversight and accountability. The NYPD used private and federal funds, without any disclosure to the lawmakers we depend-on to oversee our police forces. With this unaccountable funding, the NYPD was able to deploy tools like facial recognition, X-Ray vans, automated license plate readers, and "stingrays," fake cell towers that collect sensitive location and communications data.[1] Like many of the NYPD's new tools, stingrays spy not only on the target of an investigation, but also on untold numbers of innocent bystanders.[2]

Let me be clear, the POST Act does not prohibit the NYPD from using new surveillance tools. Rather, it merely secures this Council's indispensable role in reviewing when and how such tools are deployed. Under the POST Act, the NYPD must issue an "impact and use policy" report when choosing to use a new surveillance tool.[3] This report must describe the technology, rules, and guidelines for the use of that technology, and safeguards for protecting any data collected.[4] The City Council and the people of New York City would then be allowed to provide feedback on such an acquisition.[5] Thus, the POST Act strikes a delicate balance, requiring sufficient information to ensure oversight, while protecting operational details, sources, and methods.

Civilian oversight of policing and intelligence gathering is not only a fundamental American value, it is essential for effective policing. As then-President Obama's Task Force on 21st Century Policing found, "[l]aw enforcement agencies should establish a culture of transparency and accountability in order to build public trust and legitimacy."[6] The NYPD's current procurement methods are not only undemocratic, but they harm the NYPD's very mission of promoting public safety

(I) Impact on Muslim New Yorkers

Warrantless surveillance poses a threat to all New Yorkers, but we know that communities are not policed equitably. The POST Act will offer particularly powerful protection for our Muslim neighbors. For years, Muslim New Yorkers have faced a pattern of unjust and unconstitutional NYPD

---

[1] Joseph Goldstein, *New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says*, N.Y. TIMES, Feb. 11, 2016, https://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html.
[2] *Id.*
[3] N.Y. CITY COUNCIL 1482 § 1 (N.Y. 2017), ch. 1, 14 ADMIN. CODE OF N.Y.C. § 14-167(b) (as proposed)
[4] *Id.* at 14-167(a) (as proposed)
[5] *Id.* at 14-167(e-f) (as proposed)
[6] PRESIDENT'S TASK FORCE ON 21ST CENTURY POLICING, FINAL REPORT OF THE PRESIDENT'S TASK FORCE ON 21ST CENTURY POLICING 12 (2015), https://cops.usdoj.gov/pdf/taskforce/taskforce_finalreport.pdf.

surveillance. Specifically, the NYPD's Intelligence Division engaged in extensive, suspicionless surveillance of majority Muslim neighborhoods and Muslim families.[7] Additionally, NYPD officials have conducted blanket surveillance of entire mosques, surveilling men, women, and children for nothing more than practicing their faith.[8] Some local businesses have even been classified as "place[s] of concern" for nothing more than having customers of middle eastern descent.[9]

In addition, Muslim New Yorkers who opened their doors to law enforcement, hoping to help their community, frequently were rewarded with suspicion and surveillance. In one example, Sheikh Reda Shata welcomed FBI agents and NYPD officers into his mosque, trying to build a bridge between the community and law enforcement, but was nonetheless monitored by an undercover police officer.[10]

Muslim New Yorkers who are targeted for their faith often self-censor or pull back from their religious practices. Although most Muslim New Yorkers continue to unapologetically practice their faith in the face of police harassment, some have stopped attending their places of worship.[11] Those who continue to attend services face frequently insurmountable barriers to building trust with those around them, knowing that a friendly co-congregant may secretly be an undercover officer.[12] Other New Yorkers are afraid to practice their faith as they'd wish, refraining from wearing a beard, a headscarf, or other visible signifiers of their religion.[13] Moreover, Muslim faith leaders often speak guardedly to their congregations, fearful that an out-of-context statement, or even speaking a disfavoured dialect, might spark an investigation.[14]

Muslim student groups have also faced widespread and discriminatory surveillance. New York's Muslim Student Associations have been targeted with informants and undercover officers for as little as organizing a rafting trip[15] or having members deemed "politically active."[16] One reason why the

---

[7] Matt Apuzzo & Joseph Goldstein, *New York Drops Unit That Spied on Muslims*, N.Y. TIMES, Apr. 15, 2014, https://www.nytimes.com/2014/04/16/nyregion/police-unit-that-spied-on-muslims-is-disbanded.html?_r=0; *see also* DIALA SHAMAS & NERMEEN ARASTU, MUSLIM AM. CIVIL LIBERTIES COAL., CREATING LAW ENF'T ACCOUNTABILITY & RESPONSIBILITY & ASIAN AM. LEGAL DEF. & EDUC. FUND, MAPPING MUSLIMS: NYPD SPYING AND ITS IMPACT ON AMERICAN MUSLIMS 10 (2013), https://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

[8] Apuzzo & Goldstein, *supra* note 7.

[9] Adam Goldman & Matt Apuzzo, *NYPD: Muslim Spying Led to No Leads, Terror Cases*, ASSOCIATED PRESS, Aug. 21, 2012, https://www.ap.org/ap-in-the-news/2012/nypd-muslim-spying-led-to-no-leads-terror-cases.

[10] Eileen Sullivan, *NYPD Spied on Anti-terror Muslim Leader as He Dined with Bloomberg*, NBC NEWS, Oct. 6, 2011, https://www.nbcnews.com/id/44796663/ns/us_news-life/t/nypd-spied-anti-terror-muslim-leader-he-dined-bloomberg/.

[11] SHAMAS & ARASTU, *supra* note 7, at 12-14.

[12] *Id.* at 18.

[13] *Id.* at 15-18.

[14] *Id.* at 18.

[15] Chris Hawley, *NYPD Monitored Muslim Student All over Northeast*, ASSOCIATED PRESS, Feb 8. 2012, https://www.ap.org/ap-in-the-news/2012/nypd-monitored-muslim-students-all-over-northeast.

[16] N.Y. POLICE DEP'T, NYPD INTELLIGENCE DIVISION: STRATEGIC POSTURE 2006 17 (2006), https://www.nyclu.org/sites/default/files/releases/Handschu_Exhibit7b_%28StrategicPostureredacted%29_2.4.13.pdf.

POST Act is so crucial is that many of the most invasive NYPD programs have never produced a single lead, let alone stop a terrorist act.[17] Yet these same technologies and tactics, whose rewards are so nebulous, have a very clear cost.

Students who later learn they were targeted can suffer lasting psychological harm and life-long struggles with trust and self-censorship.[18] One Muslim student at Hunter College said that many fear that political engagement will result in being spied on.[19] Another CUNY student spoke of how she feels she doesn't know who to trust anymore.[20] At Brooklyn College, following revelations of NYPD surveillance on campus, attendance of Islam Awareness Week events plummeted.[21] One CUNY student withdrew from Muslim Student Association events after police came to his home to question him about his political opinions.[22] While the worst documented abuses may have ceased with the disbandment of the NYPD's "Demographics Unit," many Muslim students still fear speaking in class about political issues, worried that they will be misinterpreted and investigated.[23] Younger students have not been immune to this. Some educators have sought Know-Your-Rights workshops to quell student fears of surveillance for children as young as eleven.[24]

These tragic accounts are not anomalies, they reflect an ongoing pattern of discriminatory police conduct. According to the most-recent, publicly-available data from the Office of the Inspector General for the NYPD ("OIG"), over 95% of recent NYPD political and religious investigations targeted Muslim individuals and organizations.[25] The pattern of discriminatory surveillance is completely at odds with the fact that the overwhelming majority of terrorist attacks in the United States are committed by right-wing extremists and white supremacists. Let me repeat that fact, since it is so often lost in our media environment: right-wing extremists and white supremacists commit the overwhelming majority of terrorist attacks in the United States.

Amazingly, in some white supremacist attacks, their victims face greater scrutiny than the attackers. Recently, when four members of the Proud Boys, a known white supremacist organization, violently assaulted protestors in the Upper East Side, the Manhattan District Attorney's Office took the

---

[17] Goldman & Apuzzo, *supra* note 9.
[18] WATCHED (The Shorts Collective, LLC 2017).
[19] SHAMAS & ARASTU, *supra* note 7, at 23.
[20] *Id.* at 42.
[21] *Id.*
[22] *Id.* at 43.
[23] *Id.* at 44-45.
[24] *Id.* at 43.
[25] OFFICE OF THE INSPECTOR GEN. FOR THE N.Y. POLICE DEP'T, N.Y. CITY DEP'T OF INVESTIGATION, AN INVESTIGATION OF NYPD'S COMPLIANCE WITH RULES GOVERNING INVESTIGATIONS OF POLITICAL ACTIVITY 1 n.1 (2016), https://www1.nyc.gov/assets/oignypd/downloads/pdf/oig_intel_report_823_final_for_release.pdf. In its investigation, the OIG reviewed a random selection of 20% of cases closed or discontinued between 2010 and 2015 of each case type. *Id.* at 14.

extraordinary step of using a so-called "Reverse Search Warrant."[26] A Reverse Location Search Warrant allows law enforcement to gather the location data on people in an entire area at one time.[27] Alarmingly, prosecutors didn't use this Orwellian tactic to find the Proud Boys, they used it to find the protestors the Proud Boys assaulted.[28] In the end, this digital dragnet did not return information the DA's Office was looking for, instead, it was used to surveil two individuals who ended up being innocent bystanders.[29]

In contrast to the undercover practices documented above, the novel NYPD surveillance practices governed by the POST Act often are completely invisible to the target, making them much more dangerous to our freedom of speech and religion. The need for oversight is only heightened by the NYPD's clear track record of disregarding those few existing restrictions on surveillance of protected First Amendment activity. According to the OIG, over half of NYPD intelligence investigations continued even after the legal authorization for them expired.[30] Also, the OIG found that the NYPD frequently violated legal guidelines governing these investigations in other ways, such as through its use of boilerplate language in undercover officer authorization forms.[31]

(II) Impact on Immigrant Communities

In addition, these spy tools pose a particularly potent threat to our immigrant communities. All too often, these systems create a risk of information sharing with federal agencies…even ICE. For example, the NYPD has contracted for years with the private firm Vigilant Solutions, which operates a nationwide database of over 2 billion license plate data points.[32] Shockingly, last year we learned that that Vigilant Solutions was not just contracting with local police departments…it was also contracting with ICE.[33] This one vendor is responsible for recording at least one million license plates per day.[34]

---

[26] Albert Fox Cahn, *Manhattan DA Made Google Give Up Information on Everyone in Area as They Hunted for Antifa*, THE DAILY BEAST, Aug 13, 2019, https://www.thedailybeast.com/manhattan-da-cy-vance-made-google-give-up-info-on-everyone-in-area-in-hunt-for-antifa-after-proud-boys-fight?ref=scroll.

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] OFFICE OF THE INSPECTOR GEN. FOR THE N.Y. POLICE DEP'T, *supra* note 25, at 1.

[31] *Id.* Such conduct undermines the ability of independent bodies to effectively review police compliance with legal guidelines. *Id.* at 2.

[32] *See* ROCCO PARASCONDOLA, *Exclusive: NYPD will be able to track fugitives who drive past license plate readers across the U.S.*, N.Y. DAILY NEWS, Mar. 02, 2015, https://www.nydailynews.com/new-york/nypd-track-fugitives-drive-license-plate-readers-article-1.2133879.

[33] The Domain Awareness System collects the license plate data scanned by the approximately 500 license plate readers operated by the NYPD and combines it with footage from cameras and other surveillance devices around the city. The NYPD holds on to the license plate data for at least five years regardless of whether a car triggers any suspicion. *See* MARIKO HIROSE, *Documents Uncover NYPD's Vast License Plate Reader Database*, ACLU, Jan. 25, 2016, https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-reader-database?redirect=blog/speak-freely/documents-uncover-nypds-vast-license-plate-reader-database.

[34] *See id.*

Perhaps most disturbingly, the NYPD relies on Vigilant Solution's artificial intelligence to map out social networks, label New Yorkers as "criminal associates", and create databases based on the company's unproven algorithms.[35] This is just one example of countless surveillance tools that requires a systematic solution.

(III) The "Gang" Database

Additionally, the POST Act enables the public to better understand the surveillance systems that have been targeted at communities of color. For decades, the NYPD's discriminatory "Stop and Frisk" policy racially profiled New Yorkers of color, stripping them of their most fundamental rights because of the color of their skin. While New York has largely curtailed that unconstitutional blight, we continue to maintain police policies that subject New Yorkers of color to invasive, unjustified, and dehumanizing surveillance. One of the most disturbing systems is the "gang database."

As advocates made clear last week, the NYPD's gang database is little better than high-tech "Stop and Frisk." Rather than stopping racial profiling, the NYPD simply shifted from physical pat-downs to electronic searches—adding eleven New Yorkers to their sprawling database every single day.[36] The gang database treats New Yorkers as criminals just for how they dress and where they live. Children and teenagers report that the constant surveillance is so traumatic that they are sometimes afraid to leave their homes and socialize with their friends, terrified of falsely being labeled as a "gang member."

As with other forms of NYPD surveillance, the evidence of bias is overwhelming. The definition of "gang"[37] should include everyone from the mafia to white supremacists, but the database remains ninety-nine percent New Yorkers of color.[38] When you look at how the database is actually compiled, this discrepancy is no surprise. Leaked NYPD training documents show officers trained to systematically profile people of color as "gang-affiliated."[39] The NYPD includes numerous New Yorkers simply for wearing a suspicious color of clothing or just being in the same neighborhood as a suspect.[40]

(IV) Body-Worn Cameras

Alarmingly, we see the same pattern of over surveillance extend to the technologies that were sold to the public as a way to restrain and reform the police. Take body-worn cameras, which were

---

[35] *See id.*

[36] *See*, Alice Speri, *New York Gang Database Expanded by 70 Percent Under Mayor Bill de Blasio*, THE INTERCEPT (June 11, 2018) https://theintercept.com/2018/06/11/new-york-gang-database-expanded-by-70-percent-under-mayor-bill-de-blasio/.

[37] *See, Gangs and Crews of New York*, THE INTERCEPT (June 11, 2018) https://theintercept.com/document/2018/06/11/gangs-and-crews-of-new-york/.

[38] *Oversight – NYPD's Gang Takedown Efforts: Hearing Before the Comm. on Pub. Safety*. 2018 Leg., 2018-2021 Sess. at 32 (N.Y.C 2018) (statement of Dermot Shea, NYPD Chief of Detectives) [hereinafter *Oversight Hearing*].

[39] *See, Gangs and Crews of New York*, THE INTERCEPT (June 11, 2018) https://theintercept.com/document/2018/06/11/gangs-and-crews-of-new-york/.

[40] *Oversight Hearing*, at 25 (statement of Dermot Shea, NYPD Chief of Detectives).

promised to be a tool of increased accountability and justice, but which have fallen short of that promise.

Bodycam adoption was initially driven by police use of force, particularly the 2014 police killings of Eric Garner, Michael Brown, Tamir Rice, and many others. Initial evaluations offered the tantalizing promise that bodycams could increase "officer professionalism, helping agencies evaluate and improve officer performance, and allowing agencies to identify and correct larger structural problems within the department."[41] Mayor de Blasio cited these justifications when expanding the NYPD bodycam program, promising to make New York City "fairer, faster and grow trust between police and communities."[42]

Lax departmental policies allow NYPD officers untenable discretion over when and what to record.[43] At the same time, department officials have exercised their own discretion to shield officers from unfavorable footage, while quickly releasing videos that support their narrative. The net result are cameras that are less a tool to restrain cops and more a facet of public surveillance.

The public privacy impact is exacerbated by the NYPD's growing use of facial recognition and other forms of biometric surveillance. These technologies allow the police to turn a walk down the block into a warrantless search of thousands of New Yorkers.[44] The thought is disturbing, but it is even more alarming when one contemplates the use of such technology near political protests, health care facilities, an alcoholics anonymous meeting, or anyplace else where New Yorkers have heightened privacy concerns.

Sadly, the department's track record with prior bodycam policies further undercuts public confidence. Earlier this year, the Civilian Complaint Review Board said approximately 40% of requests[45] for bodycam video were unfulfilled. Alarmingly, in more than 100 cases, the NYPD falsely claimed there was no video when there actually was footage.[46] In addition, the NYPD has repeatedly been denounced by advocates for failing to abide by existing disclosure requirements, such as those

---

[41] *See* Cmty. Oriented Policing Servs. & Police Exec. Research Forum, *Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned* 5 (2014), https://www.justice.gov/iso/opa/resources/472014912134715246869.pdf.

[42] Thomas Tracy, *De Blasio Pushing for Every Cop, Detective on Patrol to Wear a Body Camera by Year's End*, N.Y. Daily News (Jan. 30, 2018, 7:53 PM), www.nydailynews.com/new-york/de-blasio-wear-body-camera-year-article-1.3788661.

[43] *Body-Worn Cameras*, Elec. Frontier Found., www.eff.org/pages/body-worn-cameras (last updated Oct. 18, 2017).

[44] Mark Blunden, *Police Bodycams with Facial Recognition to Pick Out Criminals from the Crowd*, Evening Standard (June 24, 2019. 8:54 AM), www.standard.co.uk/news/uk/bodyworn-cctv-cameras-to-pick-out-criminals-from-the-crowd-a4174061.html.

[45] Jeffrey Harrell, *Body Cam Backlog: NYPD Lags on Making Footage Public, Report Finds*, Brooklyn Daily Eagle (July 12, 2019), https://brooklyneagle.com/articles/2019/07/12/body-cam-backlog-nypd-lags-on-making-footage-public-report-finds.

[46] Memorandum from Olas Carayannis, Dir. of Quality Assurance and Improvement, Civilian Complaint Review Bd., to Members of the Civilian Complaint Review Bd. 2 (July 5, 2019), https://brooklyneagle.com/wp-content/uploads/2019/07/20190710_boardmtg_BWC_memo-2-1.pdf.

under New York's Freedom of Information Law and criminal and civil discovery.[47]

More alarmingly still, NYPD officials have repeatedly defended the use of facial recognition in conjunction with bodycams. Earlier this year, former NYPD Commissioner James O'Neill justified this Orwellian practice with the canard that "facial recognition technology is used as a limited and preliminary step in an investigation."[48] Sadly, this description of facial recognition bears little resemblance to NYPD realities. Officers have been documented texting a "match" to a witness and asking, "Is this the guy?"[49] This leading use of facial recognition can easily contaminate eyewitness memory, leading to misidentification and even wrongful conviction.[50] Without the POST Act, we have no way to track how bodycams are being integrated into the Department's growing array of biometric tracking programs.

(V) DNA Databases

The Post ACT would also provide greater insight into the NYPD's expansive and growing use of DNA databases.

Currently, police can coerce and trick innocent New Yorkers into handing over their genetic code. The risks are greatest for juveniles, who are least able to assert their right to refuse a DNA test. But even when young New Yorkers assert their rights, our outdated laws allow a workaround. Officers can test a discarded cigarette butt or used gum for DNA.[51]

Black and brown New Yorkers are particularly at risk as police departments increase DNA dragnets.[52] Already, our databases compromise the genetic identities of over 64,000 New Yorker's, and the numbers are only growing.

The POST Act would help us better understand the immoral and potentially unconstitutional practices that subject New Yorkers who have been cleared of a crime to an indefinite DNA line-up, increasing

---

[47] Tim Cushing, NYPD Finally Comes Up With A Body Camera Policy, And It's Terrible, Tech Dirt (Apr. 19, 2017), https://www.techdirt.com/articles/a20170416/14021937162/nypd-finally-comes-up-with-body-camera-policy-terrible.shtml

[48] James O'Neill, Opinion, *How Facial Recognition Makes You Safer*, N.Y. Times (June 9, 2019), www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html.

[49] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Georgetown Law Ctr. On Privacy & Tech., (May 16, 2019), https://www.flawedfacedata.com.

[50] *False Testimony/Confessions*, Cal. Innocence Project, https://californiainnocenceproject.org/issues-we-face/false-confessions (last visited Nov. 15, 2019).

[51] *See*, Katie Worth, *Framed for Murder by His Own DNA*, PBS (Apr. 19, 2018) https://www.pbs.org/wgbh/frontline/article/framed-for-murder-by-his-own-dna/.

[52] *See*, Jay Ransom & Ashley Southall, *'Race-Biased Dragnet': DNA From 360 Black Men Was Collected to Solve Vetrano Murder, Defense Lawyers Say*, N.Y. TIMES (Mar. 31, 2019) https://www.nytimes.com/2019/03/31/nyregion/karina-vetrano-trial.html; *see also*, Andrew Whalen, *NYPD'S 'Knock-and-Spit' DNA Database Makes You a Permanent Suspect*, (Feb. 2, 2019) https://www.newsweek.com/police-dna-database-nypd-swab-testing-collection-new-york-1326722

their risk of wrongful arrest. Such databases also provide information about an individual's entire family, compounding the concern about racially and ethnically discriminatory databases.

(VI) National Reform Movement

The POST Act is a comprehensive response, but it's also a modest one. The NYPD can continue using these tools—no matter how problematic—by complying with modest protections against waste, discrimination, and misuse. In fact, the POST Act would be one of the weakest surveillance reform bills in the country.[53] Just compare the bill to San Francisco[54] and Oakland, which banned facial recognition technology,[55] and eleven other jurisdictions that not only require disclosure of surveillance technology, but which ban such tools in the absence of civilian approval.[56] The evidence is clear, civilian surveillance oversight enhances public trust in police departments and public safety.[57]

Notably, the police response to surveillance oversight in other jurisdictions has been far milder, even as those jurisdictions enact reforms that are far more aggressive. Oakland's Surveillance and Community Safety Ordinance, one of the strongest ordinances in the nation, requires public approval for all forms of surveillance.[58] Yet the police have supported the reforms. The head of Oakland Police Research and Planning said it is "bizarre" to think there is "a world in which we don't want the public to know what we are doing or what we are doing with it."[59] The Chief of Police for Somerville, Massachusetts, which recently banned facial recognition, said civilian oversight would build trust and confidence in our force and our methods" and "strengthen the community connections that ultimately help us keep Somerville safe."[60] Crucially, this information helps to build the community trust that is clearly lacking today in New York.[61] The Oakland and Somerville police responses aren't the outliers: the NYPD is. At a time when departments view public disclosure as indispensable to public engagement, NYPD officials are making irresponsible and inaccurate claims that public disclosure is

---

[53] *See* ACLU, Community Control Over Police Surveillance, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance.
[54] *See* KATE CONGER, *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES, May 14, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.
[55] *See* EDITORIAL BOARD, *San Francisco Banned Facial Recognition. New York Isn't Even Close.* N.Y. TIMES, May 18, 2019, https://www.nytimes.com/2019/05/18/opinion/nypd-post-act-surveillance.html.
[56] *See* ACLU, Community Control Over Police Surveillance, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance.
[57] Oakland, California and Seattle, Washington have enacted similar police oversight laws without deteriorating public safety. *See id.*
[58] Sarah Holder & Tanvi Misra, *The Bay Area's Spy Camera Ban is Only the Beginning,* CITYLAB, May 13, 2019, https://www.citylab.com/equity/2019/05/government-surveillance-tools-facial-recognition-privacy/588712/.
[59] Michael Price, Opinion, *What Oakland Police Can Teach the NYPD,* AM NEW YORK, May 12, 2017, https://www.amny.com/opinion/what-oakland-police-can-teach-the-nypd-1-13624678/.
[60] City of Somerville, *New Somerville Policy First in MA to Add Controls, Require Public Transparency for Surveillance Technology*, NEWS, October 5, 2017, https://www.somervillema.gov/news/new-somerville-policy-first-ma-add-controls-require-public-transparency-surveillance-technology.
[61] Michael Price, *supra.*; City of Somerville, *supra.*

a "roadmap for terrorists and criminals."[62] It's not, and it's time for this Council to make clear that this sort of blatant fearmongering has no place in our policing discourse.

I'm grateful that the committee is addressing New Yorkers' myriad privacy concerns. Our alarm grows by the day, as emerging technologies exacerbate the threats we are only now starting to address. I hope that New York City rises to the task before it is too late.

In light of the foregoing, we urge this City Council to enact the POST Act. This legislation will provide vital transparency for the NYPD's acquisition of, and use of, surveillance technology. I thank you for giving me the opportunity to address these urgent issues, and I look forward to working with the Council to safeguard the rights of all New Yorkers in the months and years to come.

---

[62]Tina Moore & Max Jaeger, *NYPD Calls City county Plan to Reveal Anti-Terror Tactics 'Insane'*, NEW YORK POST, June 14, 2017, https://nypost.com/2017/06/14/nypd-calls-city-council-plan-to-reveal-anti-terror-tactics-insane/.

ATTACHMENT A

October 31, 2019

NYC Council Speaker Corey Johnson
City Hall Office
New York, NY 10007
via U.S. Mail and Email

Re: Passage of POST Act, Int. No. 0487-2018.

Dear Speaker Johnson,

We, the undersigned civil rights and community-based organizations, write to urge you to support passage of The Public Oversight of Surveillance Technology ("POST") Act – Int. No. 0487-2018.

The POST Act addresses the long-unmet need for civilian oversight of NYPD surveillance practices, particularly the acquisition and deployment of novel, highly-invasive technologies. For years, the NYPD has built up an arsenal of spy tools on the public tab while trying to block public notice and debate. These tools not only include the so-called "gang database," but also items like facial recognition, IMSI catchers (so-called "stingrays"), and automated license plate readers that can monitor a vehicle's location throughout the city.

These tools pose a privacy threat to all New Yorkers, but they pose a particularly potent threat to our immigrant communities and New Yorkers of color. Unchecked, the growing use of surveillance technology threatens to obscure and automate racial inequalities under the guise of unbiased computer systems. And too often, these systems create a risk of information sharing with federal agencies, including Immigrations and Customs Enforcement ("ICE").

For example, the NYPD has contracted for years with the private firm Vigilant Solutions, which operates a national database of over 5 billion license plate data points.[1] Shockingly, in recent years, we learned that Vigilant Solutions was not just contracting with local police departments, it was also contracting with ICE.[2] This is the vendor that the NYPD uses to record countless New Yorkers' license plates per day, and we do not have an accurate understanding of how the NYPD may be sharing license plate data with ICE.[3]

Even worse, the NYPD relies on Vigilant Solutions' artificial intelligence to map out social networks, label New Yorkers as "criminal associates," and create databases based on the company's unproven algorithms.[1] This is just one example of countless surveillance tools that requires a systematic solution.

---

[1] *See* Rocco Parascondola, *Exclusive: NYPD will be able to track fugitives who drive past license plate readers across the U.S.*, N.Y. Daily News, Mar. 02, 2015, https://www.nydailynews.com/new-york/nypd-track-fugitives-drive-license-plate-readers-article-1.2133879.

[2] Russell Brandom, *"Exclusive: ICE is about to start tracking license plates across the US."* The Verge, January 26, 2018, https://www.theverge.com/2018/1/26/16932350/ice-immigration-customs-license-plate-recognition-contract-vigilant-solutions.

[3] *See* Mariko Hirose, *Documents Uncover NYPD's Vast License Plate Reader Database*, ACLU, Jan. 25, 2016, https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-reader-database.

[1] *See id.*

The POST Act is not just a comprehensive response, but also a modest one. The NYPD can continue using these tools by complying with limited protections against waste, discrimination, and misuse. In fact, the POST Act would be one of the most limited surveillance reform bills in the country,[2] especially when viewed in comparison to San Francisco's[3] and Oakland's[4] oversight legislation, which also contain outright bans on facial recognition technology or to Massachusetts's state-wide moratorium on facial recognition.[5] Additionally, many of the jurisdictions require legislators to approve each and every surveillance system their municipality buys, unlike the POST Act, which only requires public notice.

The measure is not just widely supported by your City Council colleagues, it's even endorsed by the New York Times.[6] The message is clear: civilian oversight of surveillance enhances the public's trust in police departments and public safety.[7] Now, with twenty-seven city council members and the Public Advocate signed on as POST Act cosponsors, the time is long overdue for a hearing before the Public Safety Committee and a vote of the full City Council.

As the leader of the Council, you've constantly acted as a champion for communities in need. We urge you to do so once again and join this growing, national movement. With your support, we know the POST Act can be enacted before the end of the year. We look forward to your reply and assistance.

Cc: Chair Donovan Richards
Council Member Vanessa Gibson

Sincerely,

1. A New PATH
2. ACLU
3. African Communities Together
4. AI Now Institute
5. Albuquerque Center for Peace and Justice
6. American-Arab Anti-Discrimination Committee
7. Arab American Institute
8. Asian American Federation
9. Asian American Legal Defense and Education Fund (AALDEF)
10. Brennan Center for Justice at NYU School of Law
11. Brooklyn College - Policing and Social Justice Project
12. Brooklyn Community Bail Fund
13. Brooklyn Defender Services
14. Center for Human Rights and Privacy

---

[2] See ACLU, Community Control Over Police Surveillance,https://www.aclu.org/issues/privacytechnology/surveillance-technologies/community-control-over-police-surveillance.

[3] See Kate Conger, San Francisco Bans Facial Recognition Technology, N.Y. TIMES, May 14, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

[4] Sarah Ravani, Oakland bans use of facial recognition technology, citing bias concerns, San Francisco Chronicle, July 17, 2019, https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php

[5] See Editorial Board, San Francisco Banned Facial Recognition. New York Isn't Even Close. N.Y. Times, May 18, 2019. https://www.nytimes.com/2019/05/18/opinion/nypd-post-act-surveillance.html.

[6] *See* Massachusetts Senate, Bill S.1385, https://malegislature.gov/Bills/191/S1385.

[7] Oakland, California and Seattle, Washington have enacted similar police oversight laws without deteriorating public safety. *See id.*

15. College and Community Fellowship
16. Color Of Change
17. Columbia Journal of History
18. Constitutional Alliance
19. Council on American-Islamic Relations New York Chapter
20. Cryptoparty Ann Arbor
21. Data Law Society, Benjamin N. Cardozo School of Law
22. Defending Rights & Dissent
23. Demand Progress
24. Dignity and Power Now
25. DRUM- Desis Rising Up and Moving
26. Empire State Indivisible
27. Families for Freedom/ Familias por la Libertad
28. Families Rally for Emancipation and Empowerment
29. Fight for the Future
30. Free Press Action
31. Hacking//Hustling
32. Immigrant Defense Project
33. Inner-City Muslim Action Network
34. Jewish Voice for Peace-New York City
35. JustLeadershipUSA
36. Legal Aid Society of NYC
37. Lucy Parsons Labs
38. Martinez Street Women's Center
39. Media Alliance
40. MediaJustice
41. Million Hoodies Movement for Justice
42. MinKwon Center for Community Action
43. mother's against wrongful convictions
44. NAACP Legal Defense and Educational Fund, Inc.
45. National Lawyers Guild - NYC Chapter
46. Nevius Legal
47. New York Civil Liberties Union
48. New York Communities for Change
49. New York Immigration Coalition
50. Northern New Jersey Jewish Voice for Peace
51. NYC Privacy Board Advocates
52. Oakland Privacy
53. PDX Privacy
54. Restore The Fourth
55. Revolutionary Love Project
56. Rhode Island Rights
57. S.T.O.P. - The Surveillance Technology Oversight Project
58. Secure Justice
59. TAKE ON HATE – NY
60. Temple Beth El
61. Tenth Amendment Center
62. The Bronx Freedom Fund
63. The Calyx Institute
64. The Cypurr Collective
65. The Interfaith Center of New York
66. The National Action Network
67. Urban Justice Center
68. Urban Justice Center Mental Health Project
69. WITNESS
70. X-Lab

NYCDS

Testimony of

Sergio De La Pava

Legal Director

New York County Defender Services

Before the

Committee on Public Safety

Intro. 487-2018

The Public Oversight of Surveillance Technology (POST) Act

December 18, 2019

My name is Sergio De La Pava and I am the Legal Director at New York County Defender Services (NYCDS), a public defense office that represents tens of thousands of New Yorkers in Manhattan's criminal courts every year. I have been representing clients accused of crimes in this city for more than twenty years. Thank you to Chair Richards for holding this hearing on the POST Act, a critical piece of legislation that NYCDS strongly supports.

Police are surveilling all of us using invasive new technologies to an extent previously unimagined.[1] Defense attorneys stand as the front line of defense for our clients against the state. Yet what we currently receive in terms of disclosure from prosecutors and NYPD about existing technology and its use is, we believe, merely the tip of the iceberg. In order for people accused of crimes to fully understand and dispute the charges against them, we must have transparency about the kinds of technology that exist and how they are used. The POST Act would require the NYPD to publicly disclose this information to the benefit of our entire society, not just those accused of crimes.

---

[1] Jon Schuppe, *Amazon is developing high-tech surveillance tools for an eager customer: America's police*, NBC NEWS, Aug. 8, 2019, available at https://www.nbcnews.com/tech/security/amazon-developing-high-tech-surveillance-tools-eager-customer-america-s-n1038426.

We believe the POST Act is a critical first step in protecting communities from surveillance overreach. But it should not be the last. The City Council must also investigate other city entities that are using public money to surveil residents, such as the Department of Correction, and fund technology upgrades for defenders to create a more level-playing field between police and accused people.

Here are the kinds of surveillance technology we do know exist[2]:

- Facial recognition technology
- Video analytics
- Social media monitoring
- Gang database
- Predictive policing
- Stingrays, also known as "cell site simulators" or "IMSI catchers"
- Automated license plate readers
- Domain awareness system
- Drones
- X-ray vans
- Cameras located all over the city

We know these types of surveillance technology are used against our clients and their communities, but we do not know how they are implemented by the NYPD. We do not even know how frequently these technologies are involved in a given criminal case because we receive limited pre-trial discovery. While we hope to have a better sense of the extent of their use after the new discovery reform goes into effect in January 2020, we still will not have access to the underlying policies and procedures without passage of this bill.

New technology: Voice recognition technology

We recommend the Council consider amending the POST Act to require that other city offices or agencies disclose their use of surveillance technology as well. In particular, we recently learned that our clients detained on Rikers Island are now required to record their voice to enroll in a voice surveillance system if they want to make phone calls to their attorney or loved ones.

This voice recognition technology is being used against our clients and members of the public alike:

> In New York and other states across the country, authorities are acquiring technology to extract and digitize the voices of incarcerated people into unique biometric signatures, known as voice prints. Prison authorities have quietly enrolled hundreds of thousands of incarcerated people's voice prints into large-scale biometric databases. Computer algorithms then draw on these databases to

[2] *See* Brennan Center, *New York City Police Department Surveillance Technology*, Oct. 4, 2019, available at https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology.

identify the voices taking part in a call and to search for other calls in which the voices of interest are detected. Some programs, like New York's, even analyze the voices of call recipients outside prisons to track which outsiders speak to multiple prisoners regularly.[3]

We fear that this technology is being used by DOC, in conjunction with NYPD, for law enforcement investigative purposes, without a warrant and without consent from our clients and their loved ones. The POST Act should be amended to ensure that *all* law enforcement technology, whether used by NYPD, DOC, or any other government agency, is fully disclosed to the public.

Increase access to technology for accused people

As the NYPD ramps up its reliance on technology to surveil New York City residents, the City Council must ensure that defenders are equipped with the technology we need to defend our clients' rights and serve as a check on governmental overreach.

The Legal Aid Society has a digital forensics unit that was recently highlighted in the New York Times.[4] The unit has invested $100,000 in technology that allows defenders to make precise copies of computer drives or a person's phone in a format that holds up in court. This technology is critical to preserve evidence that may exonerate an accused person. But smaller defender offices like ours, who still represent thousands of clients every year but operate on a far lesser budget, do not have access to such tools.

Example:

The NYPD is increasingly relying on facial recognition to identify people alleged to have committed crimes on the subways. They take a still photo of someone on the train and attempt to "match" that photo with a photo of someone already in their database. Facial recognition technology has a 20-30% error rate for people of color, according to some studies.[5] Imagine our client is accused but insists they are innocent. There is evidence on their phone that they were not anywhere near the subway at the time of the alleged crime, but it is trapped in their phone.

In a situation like this, we need to not only know the algorithms and science that underlie the facial recognition technology that police relied on to make the match, but we also need to have tools to aggressively challenge those allegations in court. In short, we strongly support the passage of the POST Act, but we recommend that it be extended to include other city agencies and that the Council begin to study the other ways that technology is being improperly used against communities of color and how best to fight back.

If you have any questions about my testimony, please contact me at sdelapava@nycds.org.

---

[3] George Joseph & Debbie Nathan, *Prisons across the U.S. are quietly building databases of incarcerated people's voice prints*, THE INTERCEPT, Jan. 30, 2019, available at https://theintercept.com/2019/01/30/prison-voice-prints-databases-securus/.

[4] Kashmir Hill, *Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone.* N.Y. TIMES, Nov. 22, 2019, available at https://www.nytimes.com/2019/11/22/business/law-enforcement-public-defender-technology-gap.html.

[5] See, e.g., Steve Lohr, *Facial recognition is accurate, if you're a white guy*, N.Y. TIMES, Feb. 9, 2018, available at https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

Youth
Justice
Board

A Program of the Center for Court Innovation

520 Eighth Avenue, New York, New York 10018
p. 646 386 3100
courtinnovation.org

Dee Mandiyan, Program Manager

Testimony of the Youth Justice Board
A program of the Center for Court Innovation
before
The New York City Council
Committee on Public Safety
regarding
Proposed Int. No. 0487-2018
Creating comprehensive reporting and oversight of NYPD surveillance technologies.
December 18, 2019

Youth Justice Board

A Program of the Center for Court Innovation

520 Eighth Avenue, New York, New York 10018
p. 646 386 3100
courtinnovation.org

Dee Mandiyan. Program Manager

Digital Surveillance and Privacy

The Youth Justice Board is an after-school leadership development program that gives young people a voice in public policies that affect their lives. During their current program cycle, which runs from fall 2018 through the summer 2020, members are focusing on the digital surveillance and privacy of teens in New York City, particularly when young people interact with the justice system.

The Board spent several months researching how youth use social media, and when that use intersects with the justice system. Through interviews, site visits, and focus groups, the Board developed nine recommendations for city agencies and elected officials for supporting youth, minimizing justice system involvement, and preventing the criminalization of youth and misinterpretation of their actions on social media.

Inadequate Regulations

Government is playing catch up in the digital rights sphere, and residents face consequences without guaranteed rights or accountability.

PROBLEM	RECOMMENDATION
City Services There is no data on how often the social media actions of NYC residents become relevant to their receipt of city services (education, housing, child protective services, police involvement, etc.)	New York City Council require all agencies to report the use of social media in service provision.
Minors' Privacy There are few regulations protecting minors' data privacy outside of school, and no single-stop for youth to refer to their own rights and protections.	New York City Council draft and ratify a Youth Bill of Rights that includes clear protections for youth online.
Law Enforcement NYPD is not transparent about its surveillance practices and tools and has, in the past, violated state and federal law regulating surveillance of residents.	New York City Council require NYPD and all subdivisions to be transparent about surveillance tactics and technology; seek Council approval for purchases; include plans for data use, maintenance, and disposal; and share risk-assessment thresholds with the public.

Gang Database

The NYPD Criminal Group Database (gang database) uses both social media surveillance and real space surveillance to designate individuals as gang members.

PROBLEM	RECOMMENDATION
Targeting Youth of Color The criteria used to place young people in the database are vague, overlap with typical youth behavior, and unfairly target youth of color.	The City abolishes the Database and introduces additional measures to prevent similar tools from proliferating.
Impact on Prosecution Inclusion in the database has a significant negative impact on how a defendant is treated and prosecuted.	NYPD is prohibited from sharing unsubstantiated information about minors with other parties, such as the Federal Bureau of Investigations, Bureau of Alcohol, Tobacco, Firearms, and Explosives, Immigration and Customs Enforcement, or federal prosecutors.
Public Knowledge Information about the database—that it exists and how it impacts people—is not readily available to the public.	NYPD issues a statement that accurately describes the gang database to the public, including the number of people on the database every month since its creation, number of minors on the database at each of the above stated points in time, number of people identified as non-white, and neighborhoods represented in the database by percentage and number.

Lack of Knowledge

Youth face consequences for situations online that they do not know are wrong and that they have no guidance for handling.

PROBLEM	RECOMMENDATION
Digital Citizenship Education Public schools do not teach young people about digital citizenship and online safety, except for admonitions against cyberbullying.	New York State Education Department creates K-12 digital citizenship standards and curriculum.
Conflict Response Education Youth report that much of what they experience online is regular conflict that happens to take place through social media.	New York State Education Department implements K-12 conflict-response standards and curriculum.

To learn more about the Youth Justice Board, or to request a copy of the full report, contact Dee Mandiyan, Program Manager, at mandiyand@courtinnovation.org.

New York City Council
Committee on Public Safety

Creating Comprehensive Reporting and Oversight of NYPD Surveillance Technologies
December 18, 2019

Written testimony of
Genevieve Fried, Technology Fellow, AI Now Institute

Good afternoon Chairman Richards and members of the Committee on Public Safety. My name is Genevieve Fried and I am a Technology Fellow at the AI Now Institute, an interdisciplinary research institute at New York University that focuses on the social implications of artificial intelligence. The AI Now Institute respectfully submits the following testimony on Int. 0487, the Public Oversight of Surveillance Technology Act (POST Act).

During the 2017 Public Safety Committee hearing on this bill, the NYPD suggested that compliance with the POST Act requirements could allow adversaries to game and subvert NYPD's surveillance technology, putting New Yorkers' public safety at risk.[1] As a Computer Scientist by training with a background in the development and deployment of the machine learning and data-driven systems that drive surveillance technology, I submit the following testimony today with two goals: (1) to assure the Committee that the NYPD's claims are unfounded because the public disclosure requirements in the POST Act do not present a risk to public safety, and (2) that the POST Act is a necessary policy intervention because it provides a meaningful increase in transparency that will promote democratic oversight and will build trust between the NYPD and the communities it serves.

The POST Act Public Disclosure Requirements Do Not Present a Risk to Public Safety

Concerns that the POST Act poses a risk to public safety are unwarranted. The POST Act requires a relatively modest level of public disclosure, namely: "a description and capabilities of a surveillance technology," "rules, processes and guidelines issued by the department regulating access to or use of such surveillance technology," and "policies and/or practices relating to the retention, access, and use of data." This information provides valuable insight to the public, but is not sufficiently detailed for someone to game the system and threaten public safety.

To game a surveillance system, one would need to know far more granular details about it. At a minimum, one would need to know the specific data and datasets it uses as inputs, the systems or algorithms used to parse that data, the outputs presented by those algorithms, the strategies by which the surveillance systems are deployed, and how those strategies are implemented in practice. This type of

[1] Prendergast, D. (2017, June 18). NYPD Anti-terror Chief: Surveillance Bill Would Help Terrorists. *New York Post.* Retrieved from https://nypost.com/2017/06/18/nypd-anti-terror-chief-surveillance-bill-would-help-terrorists/; Winston, A. (2017, July 7). NYPD Attempts to Block Surveillance Transparency Law with Misinformation. *The Intercept.* Retrieved from https://theintercept.com/2017/07/07/nypd-surveillance-post-act-lies-misinformation-transparency/.

disclosure would almost certainly include schematics, design documents, and often direct access to source code and the algorithms at issue. Moreover, given that many policing technologies are not actually applied in ways that are expected or desired,[2] even knowing the strategies behind surveillance technology does not necessarily allow for gaming of that technology as operationalized by a specific agency. One would also need to know how the surveillance tool interacts with other tools that are being used and how the NYPD uses surveillance tools in connection with specific investigations or types of investigations. The POST Act does not require any of this information to be disclosed.

Far from revealing the precise manner in which someone might evade or defeat the surveillance tool, the POST Act only admits that a system is in use, which bodies have access to this system, and whether there are policies or practices in place to regulate the retention, access, and use of data. We know that this type of public disclosure does not impede the efficacy of a given surveillance tool. For example, wiretaps remain a powerful investigative tool despite widespread public knowledge of their existence and the rules governing their use.[3]

In addition, since the NYPD's statement on risk to public safety in 2017, numerous other municipalities across the country have adopted ordinances mandating the publication of far more information on surveillance technology as well as civilian oversight of police surveillance. Seattle[4] and California's Oakland,[5] Berkeley,[6] and Davis[7] have all barred municipal police from deploying new surveillance technology without approval from the city council. San Francisco adopted these measures while also banning the use of facial recognition by police altogether.[8] Though public safety concerns were raised during the deliberations of these ordinances, each measure passed unanimously or near-unanimously and now provide the public with far more information than the POST Act requires.

---

[2] Green, B., & Chen, Y. (2019). Disparate Interactions: An Algorithm-in-the-Loop Analysis of Fairness in Risk Assessments. Proceedings of the ACM Conference on Fairness, Accountability, and Transparency (FAT*). Retrieved from https://www.benzevgreen.com/wp-content/uploads/2019/02/19-fat.pdf

Bond-Graham, D., & Winston, A. (2013, October 30). All Tomorrow's Crimes: The Future of Policing Looks a Lot Like Good Branding. *SF Weekly News*. Retrieved from https://archives.sfweekly.com/sanfrancisco/all-tomorrows-crimes-the-future-of-policing-looks-a-lot-like-good-branding/Content?oid=2827968

Puente, M. (2019, March 12). LAPD data programs need better oversight to protect public, inspector general concludes. *Los Angeles Times*. Retrieved from https://www.latimes.com/local/lanow/la-me-ln-lapd-data-20190312-story.html

[3] Wiretap Reports. (n.d.). *United States Courts*. Retrieved from https://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports

[4] The Surveillance Ordinance. (n.d.). *Seattle Information Technology*. Retrieved from https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies/about-surveillance-

[5] PAC Surveillance Technology Ordinance Approved by City Council. (2018, September 13). *City of Oakland.* Retrieved from https://www.oaklandca.gov/resources/pac-surveillance-technoloy-ordinance-approved-by-city-council

[6] BondGraham, D., (2018, March 14). Berkeley Council Approves Surveillance Technology Oversight Ordinance. *East Bay Express*. Retrieved from https://www.eastbayexpress.com/SevenDays/archives/2018/03/14/berkeley-council-approves-surveillance-technology-oversight-ordinance

[7] Milne, S. (2018, March 21). Davis to Regulate Hi-Tech Surveillance. *Capital Public Radio*. Retrieved from http://www.capradio.org/articles/2018/03/21/davis-to-regulate-hi-tech-surveillance/

[8] Dastin, J. (2019, May 14). San Francisco votes to ban city use of facial recognition technology. *Reuters*. Retrieved from https://www.reuters.com/article/us-san-francisco-facial-recognition/san-francisco-votes-to-ban-city-use-of-facial-recognition-technology-idUSKCN1SK2NH

Litigation and advocacy in other jurisdictions has also required local law enforcement to publicly release more detailed information about surveillance technologies than required by the POST Act. For example, earlier this month the City of New Orleans was ordered to comply with a public records request regarding the locations of the City's surveillance cameras.[9]

To date, there has been no evidence that the public disclosure required by municipal ordinances or litigation has resulted in any public safety threats.

The POST ACT Promotes Democratic Oversight and Public Trust

The stakes of municipal surveillance technology are incredibly high.[10] An important aspect of this technology is its wide scope: many people, even those who are not and never will be under investigation, can be tracked and affected by these systems. There is no functional way to opt-out. For instance, New Yorkers who do not want to be tracked by one of the at least 20,000 cameras around New York City that connect to the NYPD's Domain Awareness System[11] would have to avoid going into the city. In some cases, this inability to opt-out poses additional risks to an individual or community's safety and sense of belonging. For instance, the surveillance technology commonly known as Stingrays mimic cell site towers to allow the NYPD to identify a person's cell phone location. This interferes with the ability for all cellphones in the vicinity to connect with actual cell site towers, which means that when a Stingray is deployed, individuals in its range will not be able to make or receive calls, including calls to emergency services. Even if such disruption is temporary, it can have serious consequences.

Communities of color and low-income New Yorkers are the most vulnerable to this type of pervasive surveillance. A history of racialized policing practices in New York City raises concerns that surveillance technology will disproportionately burden the urban poor and minorities. NYPD's in-house predictive policing system raises this concern.[12] The algorithms underlying predictive policing systems learn patterns based on historical crime data. Yet as researchers and advocates have demonstrated, this data reflects not the prevalence of crime but rather policing practices and policies.[13] This is particularly true in

---

[9] In Win For Civil Rights Groups and Public Defenders, Appeals Court Orders New Orleans to Turn Over Surveillance Camera Locations. (2019, December 6). *Southern Law Poverty Center*. Retrieved from https://www.splcenter.org/presscenter/win-civil-rights-groups-and-public-defenders-appeals-court-orders-new-orleans-turn-over

[10] Green, B. (2019, June 27). Smile, Your City Is Watching You. *New York Times*. Retrieved from https://www.nytimes.com/2019/06/27/opinion/cities-privacy-surveillance.html

[11] A Conversation with Jessica Tisch '08. (2019, July 17). *Harvard Law Today*. Retrieved from https://today.law.harvard.edu/a-conversation-with-jessica-tisch-08/

[12] 'Red Flags' as New Documents Point to Blind Spots of NYPD 'Predictive Policing'. (2019, July 15). *Daily Beast*. Retrieved from https://www.thedailybeast.com/red-flags-as-new-documents-point-to-blind-spots-of-nypd-predictive-policing

[13] Lum, K., & Isaac, W. (2016). To Predict and serve? *Significance*, 13(05). doi: 10.1111/j.1740-9713.2016.00960.x

Richardson, R., Schultz, J. M., & Crawford, K. Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. New York University Law Review Online. Retrieved from https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/

New York, where millions of stop-and-frisk encounters–a practice ruled unconstitutional in 2013–constitute the data of crime-forecasting systems.[14]

Given the stakes of police surveillance technology, there is significant value in the public having knowledge about what systems may be affecting their lives and whether the NYPD has rights-preserving safeguards in place. Yet there currently exists a dearth of information—let alone ways of accessing information—about what surveillance technology the NYPD uses. Most of what we currently know about the surveillance technologies NYPD employs is based on documentation released following costly FOIL litigation, investigative journalism, and inquiries by the criminal defense community and researchers. These efforts have shown that surveillance technologies are pervasive in New York City and that they have unfettered reach, tracking and implicating even those who are not, and may never be, under investigation.

For example, public records request revealed that the NYPD gang database under the de Blasio is massively expanding under vague and sweeping criteria that dictate inclusion in the database. Marne Lenox, an attorney at the NAACP Legal Defense and Educational Fund, described this system as "criminalizing friendships."[15] Individuals do not receive notification when they are added to the database and there are no clear processes to challenge one's inclusion in it. The NYPD has not clarified fundamental questions such as how the database is maintained and purged, nor who has access to it. Several organizations have filed public records requests to find out more, which the NYPD has largely evaded.

These grievances are at the heart of the motivation for the POST Act. NYPD's continual resistance to engage with transparency, denying freedom of information act requests, discovery requests, and legislation, is highly damaging. Lack of transparency impedes civil rights and liberties, but it also undermines public trust. The NYPD's opacity contributes to a climate of suspicion about what surveillance technology is actually in place and how it is used. When the public eventually learns information about the NYPD's practices or tactics, it often confirms their worst fears. A notable example are the recent revelations about the NYPD's quota system that rewarded officers for arresting Black and Latinx residents.[16] The NYPD has argued that the public should trust them to use surveillance technologies safely and lawfully,[17] but the relationship between communities and the NYPD is not strong

---

[14] Richardson, R., Schultz, J. M., & Crawford, K. Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. New York University Law Review Online. Retrieved from https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/

[15] Speri, A. (2018, June 11). New York Gang Database Expanded by 70 Percent Under Mayor Bill De Blasio. *The Intercept*. Retrieved from https://theintercept.com/2018/06/11/new-york-gang-database-expanded-by-70-percent-under-mayor-bill-de-blasio/

[16] Brown, S. R., & Rayman, G. (2019, December 5). Ex-cop details NYPD 'collar quotas' -- arrest black and Hispanic men, 'no cuffs on soft targets' of Jews, Asians, whites: court docs. *Daily News*. Retrieved from https://www.nydailynews.com/new-york/nyc-crime/ny-nypd-quotas-lawsuit-20191205-osdwj4kounf5xkvurkj3wshqry-story.html

[17] McCormack, S. (2015, October 2). NYPD Says 'Trust Us' on Potentially Dangerous X-Ray Vans Roaming the Streets of New York. ACLU. Retrieved from https://www.aclu.org/blog/privacy-technology/surveillance-technologies/nypd-says-trust-us-potentially-dangerous-x-ra

enough for this approach to be viable. It is advantageous for police-community relations for the NYPD to be more forthcoming about the surveillance technologies it uses, how that use is regulated, and how data is retained, accessed, and applied. The impact assessments mandated by the POST Act offer the opportunity to promote transparency in a way that could significantly build trust across stakeholders and could provide democratic oversight to the public—whose tax dollars pay for these systems and on whose behalf these systems are deployed.

A loss of privacy and a lack of democratic input are not the inevitable outcomes of new technology. It is up to bodies such as the New York City Council to ensure that technological innovation is grounded within public transparency and accountability. The POST Act provides a necessary measure of public disclosure to NYC residents about how they are being surveilled without posing a public security risk. This type of transparency is necessary for a robust discourse about the social utility of surveillance technology.

Thank you for your time.

---

v.

STATEMENT OF
Ras OMeil NOVado MORgan,
Plaintiff, Pro Se
17-CV-6454 MORgan vs CITY OF NEW YORK

BEFORE THE
COMMITTEE ON PUBLIC SAFETY

FOR A HEARING CONCERNING,
Int 0487-2018
A Local Law to amend the administrative code of the city
of
New York, in relation to creating comprehensive
reporting and
oversight of NYPD surveillance technologies

PRESENTED
Wednesday, December 18, 2019

Background

His Imperial Majesty Haile Selassie I, Emperor of Ethiopia. King of kings and Lord of lords Conquering Lion of the tribe of Judah, Elect of God, the Light of the World.

On June 1, 1954, His Imperial Majesty Haile Selassie First received a ticker-tape welcome during his five-day trip to New York City. The Emperor's visit to New York served as the first leg of his tour of the United States, Canada, and Mexico, intended to strengthen cultural and commercial ties between the United States and Ethiopia. In addition to the honors His Imperial Majesty received at his parade, attended by an estimated one million people, the Emperor also received tributes at the United Nations, an organization he celebrated for its achievement in repelling aggression in Korea. As descendent of King Solomon and Makeda, Queen of Sheba, His Imperial Majesty, was born Tafari Makonnen, came to power in 1916 as a leader of the Christian opposition to Lij Yasu. His Imperial Majesty led Ethiopia into the League of Nations in 1923 and in 1928 crowned king and two years later, in 1930, he officially took the throne as Ethiopia's 225th Emperor. His coronation was greeted by Jamaican followers of the prophet Hon. Marcus Mosiah Garvey as fulfillment of prophecy, which spurred the birth of the Rastafari people, who are named after His Imperail Majesty birth name.

Furthermore, on October 4, 1963 His Imperial Majesty Haile Selassie First was welcomed to New York City with a second ticker-tape parade. His Imperial Majesty addressed the United Nations on the day of his parade to call for equality and an end to racial discrimination. His Imperial Majesty pleas for safeguarding unchecked aggression and violations of human rights occurred in the midst of the Civil Rights Movement in the United States, just days before Freedom Day in Selma and a month before President John F. Kennedy's assassination

Testimony

Greetings City of New York Council Members,

I am, Ras OMeil NOVado MORgan, Plainitff, Pro Se, in MORgan vs CITY OF NEW YORK, Civil Rights Lawsuit 17-CV-6454 at EDNY. In the matter before the United States of America District Court for the *Eastern District of New York*, I am challenging the unconstitutional policies of Anti-African racial profiling, iris scanning, DNA capturing, and forceful removal of Turban, to be photographed without head covered, that was done to me by CITY OF NEW YORK POLICE DEPARTMENT Agents from false arrest on Sunday 2nd of November 2014 through Monday 3rd of November 2014. From previous Civil Rights lawsuit against CITY of NEW YORK, I know the problem is found in our United States of America Constitution Amendment 13th, which permits "slavery and involuntary servitude as punishment for crime whereof the party shall have been duly convicted". On the later, while introduced by CITY OF NEW YORK Council and referred to committee on Civil service and labor on February 14, 2018 by prime sponsor the Public Advocate (Mr. Williams), the Resolution 0181-2018 is calling upon Congress to propose an amendment to the Constitution of the United States of America Section 1 of the 13th Amendment, to prohibit slavery and involuntary servitude as a punishment for a crime needs all members support. As 2019 is 400 years since 1619 of British Colonies started enslaving Africans, the Congress passed HR1242 that was signed into law as public law 115-102.

Now to matter before this Committee, According to Surveillance Technology Oversight Project at Urban Justice Center, "For years, the NYPD has built-up an arsenal of cutting-edge,

military-grade spy tools without any public notice, debate, or oversight. The POST Act brings much-needed civilian review to NYPD policies, letting elected lawmakers know the types of surveillance conducted on New Yorkers and how that information is kept safe from federal agencies, including ICE. Existing tools include "stingrays", fake cell towers that can track New Yorkers' location and data traffic. Unlike the FBI and a growing list of police departments across the country, the NYPD has no public policy to explain how stingrays can be used, where they can be targeted, and what happens with the data from the thousands of bystanders who are caught up in their use.
Other known tools include X-ray vans that use ionizing radiation to see through walls, vehicles, and even clothing. Automatic license plate readers can monitor a car's location throughout the city, sharing that database with other agencies and private vendors. Additionally, the Domain Awareness System takes data from those tools and countless other systems to create a real-time log of millions of New Yorkers."

Additionally, On March 20th and March 23rd 2018, I emailed, which is attached here, City of New York Council Speaker Johnson, Members J. Williams now Public Advocate, A. Maisel, and V. Gibson who is one of the Post Act sponsors. In learning of the proposed bill, I wrote then that "I am writing on your proposed legislation: Int. No. 487, A Local Law to amend the administrative code of the city of New York, in relation to creating comprehensive reporting and oversight of NYPD surveillance technologies. § 14-175. Annual surveillance reporting and evaluation. I expressed then that "I have issues with NYPD Iris policy that has caused me great harm as stated in the Holy Bible KJV, Book of Revelation Chapter 14, verses 9 and 11."

Furthermore, I received email from my FOIL request with record FOIL-2018-056-00929 Criminal Justice Bureau Iris Data for dates December 31, 2010 to May 20, 2018 attached here to my statement, from openrecords@records.nyc.gov on July 27, 2018 that I forwarded, without response, to State of New York officials, City of New York Officials and Media organizations the Wall Street Journal and the New York Times.

Now, this sounds like a scene from movie *Minority Report*: The New York City Police Department is now tracking suspects by scanning their irises. City of New York police department started, without any legislation from Federal, State or Local bodies, using machines to scan the irises of prisoners in 2010. As fact, Paul J. Browne, former Police Department's chief spokesman, said then that since the beginning of 2010, the department had taken about 24,000 iris photographs. The iris scans, like fingerprints and the photographs, are kept as a part of the case file, Mr. Browne said. On the other hand, Donna Lieberman, executive director of the New York Civil Liberties Union, said she was concerned by the lack of public discourse about the new technology prior to its implementation. She said the public has no idea of the efficacy, cost or need for the process. Ms. Lieberman also raised concerned about privacy issues stating "Whenever the police start collecting personal information and start putting it in a database, we become concerned," she said.

In light of the foregoing, I urge this City Council to enact the POST Act. This legislation will provide vital transparency for the CITY OF NEW YORK Police Department acquisition of, and use of, surveillance technology. Also, I implore the Council to pass resolution 0181-2018. I give thanks for the opportunity to address these urgent issues, and I look forward to working with the Council to safe guard the rights of Rastafari New Yorkers in the months and years to come.

Blessed Love,

BROOKLYN DEFENDER SERVICES

TESTIMONY OF:

Elizabeth Daniel Vasquez – Special Forensic Science Counsel, Criminal Defense Practice

Written with Jacqueline Renee Caruana—Senior Trial Attorney, Criminal Defense Practice

BROOKLYN DEFENDER SERVICES

Presented before

The New York City Council Committee on Public Safety

Hearing on Int. 0487

December 18, 2019

My name is Elizabeth Daniel Vasquez. I am the Special Forensic Science Counsel at Brooklyn Defender Services (BDS) and lead the Forensic Practice Unit within the Criminal Defense Practice. I have practiced as a criminal defense lawyer and as a civil rights attorney in New York, Washington, DC, and in federal courts across the country. The Forensic Practice Unit's mission is to provide resource and support counsel services to trial attorneys facing complex forensic issues in misdemeanor, felony, and homicide cases in Brooklyn Criminal and Supreme Court. In that role, the Unit monitors the development of emerging scientific, technical, digital, and surveillance techniques, educates our trial lawyers regarding those techniques, and analyzes the legal and scientific or technical issues raised by the techniques themselves as well as their use or misuse.

BDS provides multi-disciplinary and client-centered criminal, family, and immigration defense, as well as civil legal services, social work support and advocacy, for over 30,000 clients in

Brooklyn every year. We thank the City Council Committee on Public Safety, and in particular Chair Vanessa Gibson, for the opportunity to testify about Int. 0487 ("POST Act"), which would bring greater transparency to the New York Police Department (NYPD)'s use and development of surveillance technologies.

The Council should act to bring the NYPD's development and use of broad-based surveillance technologies out of the shadows of secretive corporate deals and undisclosed experimentation on this city's communities of color into the light. The ground is moving at remarkable speed on these issues. The City cannot afford to wait.

I. BDS Supports Int. 0487

BDS strongly supports Int. 0487. Specifically, this crucial legislation would require annual reporting on surveillance technologies used by the NYPD. The minimal reporting required would include a description of each qualifying technology along with that technology's capabilities. The NYPD would be required to report on the usage and intra-departmental restrictions on the use of such technology, including information on court authorizations or the lack thereof. The Department would need to identify the safeguards put in place to protect the data collected, and the policies and practices implemented relating to the retention and use of the data, as well as access to the data, both internally and externally. Access to data reporting would require the NYPD to be transparent about the access available to both members of the public *and* entities outside the NYPD, including private companies and federal agencies. Finally, the NYPD would be obligated to provide a description of its internal oversight mechanisms implemented to ensure compliance with these policies, and any tests or reports regarding the health impacts of the technologies.

The POST act was originally introduced by the Council in 2017. In the two years since its initial introduction, technological advancements in surveillance have reached new levels. That progress in technical capability and growth in surveillance saturation has not been met by an evolving commitment to transparency. Instead, here in New York, the NYPD continues to insist on complete secrecy surrounding their use of surveillance technologies. The justification for this secrecy is repeatedly focused on an appeal to necessity. As the Supreme Court counseled more than 50 years ago, however, "It is said that if such . . . searches cannot be made, law enforcement will be more difficult and uncertain. But the forefathers, after consulting the lessons of history, designed our Constitution to place obstacles in the way of a too permeating police surveillance, which they seemed to think was a greater danger to a free people than the escape of some criminals from punishment." *United States v. Di Re*, 332 U.S. 581, 595 (1948).

While many Americans were alarmed in recent years by successive revelations of domestic surveillance programs by the federal government, the proliferation of powerful surveillance technologies used by state and local law enforcement agencies has received comparatively little attention. This is, in part, by design. In New York, the NYPD appears to have developed

significant technologies in house. The Department has achieved this by engaging in broad secretive partnerships with technology companies, and funding development, roll out, and use through their New York Police Foundation, instead of city contracting.[1] There has been little to no public accounting of what technologies NYPD has developed, the capabilities of those technologies, the parameters for their use, or their cost. Much of this technology, however, is also provided to police agencies pursuant to non-disclosure agreements, either by the manufacturers[2] or the federal government.[3]

Outside of the growth of surveillance technology strictly for law enforcement use, corporate collectors of big data have partnered with police agencies, expanding the dimensions of public concern. For example, it has been recently revealed that Amazon is partnering with hundreds of law enforcement agencies in the United States, by giving them access to surveillance data gathered through its "Ring" home doorbell camera system. In return for access, Amazon has asked police to actively market these devices to the community.[4] Closer to home, the NYPD apparently allowed IBM secret access to vast amounts of NYPD camera footage as part of a project to develop object identification software that would identify individuals by skin tone.[5]

Some police agencies, including the NYPD, justify this secrecy as critical to our national security, particularly as it relates to the threat of terrorism. However, just as military-grade equipment like armored vehicles sold to local police forces have been deployed at public protests, surveillance technology may be used by police in monitoring political activities. Indeed, one of the biggest potentials for abuse of surveillance technologies lies in its ability to decimate public anonymity, and thereby eradicate our cornerstone associational freedoms: the rights to free speech, assembly, and association, along with our community expectation of privacy.

Beyond the mobilization of the threat of terrorism to justify a permeating surveillance system, however, police agencies, particularly including the NYPD, have consistently used these technologies not against some looming apocalyptic threat, but instead in the service of everyday policing. And years of secrecy have allowed the NYPD to deploy these tools—without disclosure or court oversight—in investigations against our clients, particularly those facing criminal allegations and/or immigration enforcement. For example, through FOIL litigation

---

[1] Laura Nahmias, Police foundation remains a blind spot in NYPD contracting process, critics say (Jul. 13, 2017), https://www.politico.com/states/new-york/city-hall/story/2017/07/13/police-foundation-remains-a-blind-spot-in-nypd-contracting-process-critics-say-113361 (last visited Dec. 16, 2019).
[2] Kim Zetter, Police Contract With Spy Tool Maker Prohibits Talking About Device's Use Wired (2017), https://www.wired.com/2014/03/harris-stingray-nda/ (last visited Dec. 18, 2019).
[3] Juliet Linderman & Jack Gillum, Baltimore police often surveil cellphones amid US secrecy KRON4 (2015), http://kron4.com/2015/04/08/baltimore-police-often-surveil-cellphones-amid-us-secrecy/ (last visited Dec. 18, 2019).
[4] Elise Thomas, New Surveillance tech means you'll never be anonymous again (Sept. 16, 2019), https://www.wired.co.uk/article/surveillance-technology-biometrics (last visited Dec. 18, 2019)
[5] George Joseph & Kenneth Lipp, IBM used NYPD surveillance footage to develop technology that lets police search by skin color (Sept. 8, 2018), https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/ (last visited Dec. 16, 2019).

conducted by the Georgetown Center on Privacy & Technology, we now know that the NYPD has been using facial recognition technology to develop leads in everyday investigations for years and across thousands of arrests. However, I can count on one hand the number of criminal cases our office has seen in which the use of facial recognition was disclosed.

New York City is behind the curve when it comes to monitoring and regulating law enforcement use of surveillance technology. Recently, San Francisco, Berkeley, Oakland, and Somerville, Massachusetts banned the use of facial recognition software by law enforcement and government agencies. The city of Portland, Oregon is considering forbidding the use of facial recognition entirely, including by private businesses. All that the POST Act seeks to accomplish is baseline monitoring without regulation; the Act merely imposes the requirement that the NYPD report what technology it is using.

Given the disparate impact of law enforcement in general, these tools are undoubtedly used disproportionately in low-income communities of color. It is also possible that these technologies have been used without proper court authorization, potentially undermining the integrity of untold numbers of criminal convictions. However, the secrecy with which surveillance technology has been procured and implemented prevents any and all accountability. This common-sense legislation simply creates a measure of transparency so that policymakers and the public can more fairly evaluate it.

II. Surveillance & Policing in New York City: What We Know and What We Don't

It is important to understand the types of surveillance technology used by the NYPD that have been disclosed, generally as a result of lawsuits and FOIL litigation. It is also important to understand that the vast majority of police interventions in New York City are not related to counter-terrorism, but summonses and arrests for minor offenses in marginalized communities under the Broken Windows strategy. Without transparency and accountability, it is impossible for policymakers and the public to know which police activities involve invasive and sometimes costly surveillance tools, and whether any justifications offered by the NYPD are valid.

The following is an overview of some of the surveillance technology that we suspect NYPD is using but, again without passage of legislation like the POST Act, our organization and the rest of the public cannot know for sure:

The Domain Awareness System

Definition: The Domain Awareness System ("DAS") is a software program created by the NYPD and Microsoft that aggregates data collected by the NYPD across the city. DAS serves as a central repository and data analytic application for (1) video collected from private-sector security camera feeds, (2) each of the automated license plate readers placed around the city; (3) all of the NYPD's records (including complaints, summonses, arrests, reports, 911 calls, and

warrants) tagged with a geolocator; and (4) data feeds from the gunshot detectors (ShotSpotters) placed around the city. DAS provides at least three analytics functions on top of its data aggregation: (1) sensor alerting; (2) automated pattern recognition; and (3) real-time 911 call response analytics.

What we know: NYPD partnered with Microsoft beginning in 2008, and originally described the project as an information-sharing initiative arising from the 9/11 Commission's recommendations. However, according to its developers, NYPD recognized the DAS software's usefulness in general policing in 2013 and expanded the project's scope. While the project originally was only physically accessible to the Counterterrorism Bureau, in 2016, NYPD completed the software's conversion to a mobile application and deployed it on all 35,000 NYPD officer's department-issued cellphones.

DAS integrates automated license plate readers, video analytics, and Shotspotters with all of NYPD's records. The software allows officers—via their mobile phones—to access vast amounts of data about individual New Yorkers, locations, and cars. Additionally, DAS can deploy sophisticated predictive data analytics. For example, DAS's automated pattern recognition allows an officer to determine where a particular license plate of interest is likely to be at a particular time.

DAS is also used to run complex predictive policing algorithms, deploying officers based on algorithmic decision-making.

What we know that we don't know: The public has not been told the full extent of DAS's capabilities. In addition, the public has not been told exactly what type of aggregated data DAS aggregates. For example, does DAS track metrocard swipes? or does it connect to the gang database? or does it connect with records maintained by other city agencies, like the DMV or the OCME?

As criminal defense lawyers, we are not regularly seeing the searches conducted in DAS on specific cases. Discovery has not revealed the extent to which DAS is actually being used by officers in general policing.

Automated License Plate Readers

Definition: Automated license plate readers ("LPR") are devices that can be attached to poles or police cars and capture an image of every license plate that passes the device. In addition to capturing the license plate, the image taken by the reader/detector also regularly captures the entire car, the people inside the car, and portions of the surrounding roadway.

What we know: There are at least 250 mobile detectors and 50 fixed detectors covering New York City. These readers/detectors were capturing approximately 3 million images a day, as of 2017. The readers/detectors deploy optical character recognition software that allows them to alert on specifically targeted license plates. Additionally, image data aggregated from the City's

LPRs are fed into DAS and analyzed for time-and-place patterns. That aggregated data, along with the predictive forecasting of future locations, is available in DAS to every officer carrying a department-issued cellphone. Historical data is maintained for at least five years.

ShotSpotter

Definition: ShotSpotter is an acoustic gunfire detection system owned by a California-based corporation called SST, Inc. The New York City Police Department is a customer of SST, Inc, and SST has installed the ShotSpotter system at various locations throughout the city.

What we know: At the hardware level, the ShotSpotter system within the city consists of a network of acoustical sensors—consisting of a microphone, a GPS chip, and a converter chip—that are constantly "listening" and recording. ShotSpotter's acoustical sensors are constantly listening, but are only triggered to notify ShotSpotter's system when an impulsive sound registered by the sensor is categorized by an algorithm as potential gunfire. When the sensor algorithmically categorizes an impulsive sound as potential gunfire, the sensor sends an alert for possible gunshots. After a computer review, the sound is then reviewed by a human operator, who then alerts local law enforcement to the sound of possible gunshots and the system's calculated location for those gunshots.

What we know we don't know: The public does not know whether ShotSpotter is retaining spool data from its acoustical sensors that capture (or have the capability to capture) sound other than gunshots. For example, the public does not know whether the ShotSpotter system would allow SST or the NYPD to listen through the sensor in real-time or to review conversation captured by the system's microphones.

Predictive Analytics and Predictive Policing

As described above, we know that the NYPD is deploying predictive analytics and predictive policing modelling within DAS. Other instances of NYPD use of this type of big data analytics have not been disclosed.

Facial Recognition Technology

Definition: Broadly, facial recognition technology is used to compare a probe photo—typically taken as a still from surveillance footage or social media and depicting an unknown individual—against a database of still photographs depicting known individuals—typically comprised of arrest photographs, pistol license photographs, or DMV records.

What we know: Since at least 2010, the NYPD has contracted with a private vendor and developed facial recognition software for use on probe photos and against a database of known photos. Starting in 2011, the NYPD created a Facial Identification Section ("FIS") that is available for referrals from any investigation in which there is a still image of a potential face. When the NYPD's FIS runs a search, the search is set to produce a minimum of 200 hits.

What we know we don't know: Criminal defense attorneys are not being told when FIS has been used in a case. While the NYPD has reported FIS's role in almost 3,000 arrests between 2011 and 2017, we saw reporting of FIS's use during discovery in criminal cases in less than 5 of our cases.

The public is not being told how FIS's software actually functions, what its error rate is, how well it handles searches involving people of color and women, and what, if any, requirements govern when facial recognition can be used.

While the existence of FIS and static-image facial recognition software has been acknowledged, we do not know whether the NYPD has or uses real-time, facial-surveillance monitoring or datamines private photo datasets or private digital images, like those from Facebook, Instagram, and Youtube.

Social Media Monitoring

Definition: The practice of following or collecting data from social media accounts, including Facebook, Instagram, and Twitter. Social media monitoring can be targeted at a particular individual or at certain locations, associations, or message content. The technique can also take numerous forms, including methods relying solely on scrubbing publicly-available data to specifically "friending" or "following" individuals in order to gain access to private data. Furthermore, the technique can be deployed manually (by an individual investigator) or using big data analytics tools (like Dataminr or Palantir).

What we know: Criminal defense attorneys know very little about the extent to which the NYPD is using social media monitoring. Public reporting indicates that the techniques have been used to monitor protestors, as well as to allegedly identify gang members.

What we know we don't know: At this point, the public knows very little about what surveillance technologies the NYPD is using to monitor social media. The NYPD has not revealed what tools they use for social media monitoring, or what other big data analytics systems they feed social media information into. Furthermore, the NYPD has been silent about whether and how social media monitoring is used in combination with the facial recognition technology discussed above.

Criminal Group Databasing and the "Gang Database"

Definition: An aggregation of data about specified individuals allegedly suspected of gang involvement.

What we know: The gang database currently contains more than 15,000 individuals. Members of the public generally do not know that they have been included in the database, do not know on what basis they were included, and cannot challenge their inclusion, The NYPD has reported that 95% of the database is comprised of individuals of color.

What we know we don't know: The public does not know whether the gang database is connected to DAS. Similarly, the public does not know whether the NYPD has connected the gang database to other mass surveillance tools, like social media monitoring.

DNA Database Local DNA Index

Over the last decades, the Office of the Chief Medical Examiner ("OCME") has amassed a shadow, rogue DNA database housing samples from New Yorkers who had contact with the NYPD, were arrested, charged, or exonerated. It is apparent that the NYPD has access to information regarding a person's inclusion or lack of inclusion in the OCME's local database. It is also apparent that there has been some policy coordination between the NYPD and OCME surrounding the growth of the local database. The local database is extra-legal, as it contains the profiles of individuals who, by law, are ineligible for inclusion in the State's DNA database. The public has very little information regarding this coordination between NYPD and OCME or exactly how the NYPD and OCME are using this information.

BDS supports legislation on the state level to establish a single computerized state DNA identification index and require municipalities to expunge records stored in a municipal DNA identification index.[6] Senate Bill S. 6009 (A. 7818) would clarify that the index maintained by the New York State Department of Criminal Justice is the only permanent DNA identification index authorized under state law. This legislation would also prohibit local governments from maintaining DNA identification indexes and require them to expunge all improperly collected DNA samples.

In addition to this coordination with the OCME, the NYPD has also reported that it has purchased Rapid DNA testing machines. The public has not been informed why the NYPD purchased this equipment or what use it intends to put the Rapid DNA testing machines to.

Similarly, it has been publicly reported that the NYPD has also worked with Parabon Nanolabs to, at a minimum, conduct DNA phenotyping. It appears that the NYPD contracted with Parabon at a time when Parabon was not licensed by the New York Department of Health to conduct DNA testing, as required by New York law.

Other technologies

It is also clear that the NYPD is working with the MTA and that there are potential surveillance capabilities tied to both the new OMNY system and the help point kiosks installed throughout

[6] See S. 6009 (Hoylman)/ A. 7818 (Wright)

the subway system. Additionally, it has been publicly acknowledged that the NYPD owns both drones and x-ray vans.

III. How transparency in NYPDs use of technology is imperative for compliance with New York's new discovery laws

The criminal discovery reform legislation included in this year's New York State budget generally requires all evidence and information in a criminal case to be turned over within 15 days of arraignment and on an ongoing basis and mandates that prosecutors make these disclosures prior to the expiration of any plea offer. Early and complete disclosure promotes fairness in the criminal justice system. As such, the law does not limit discovery to the specified list of discoverable items. A party can request and a court can order disclosure even if it is not specified within the law as long as it is relevant to the case. The law also allows for the defense to adequately investigate a case so that even if items are not within the control or possession of the prosecutor, the defense can still move to preserve evidence or a crime scene and the defense can subpoena any additional items.

Many of these items will require the NYPD and OCME to provide evidence that, under the existing discovery regime, would often never actually be made available to the defense. Prosecutors will now be required to make efforts to communicate with NYPD and OCME to preserve and obtain documents and physical evidence. There is a due diligence requirement built into the statute. This free flow of information between the prosecutor, law enforcement, and other agencies is essential for discovery reform and compliance. The State Legislature and the New York City Council must ensure that NYPD, OCME, and other agencies providing discoverable material to the District Attorney's Office are compliant and assist the prosecution with this process.

What we have seen in Brooklyn is that Prosecutors often do not know when NYPD has used a particular surveillance technology to investigate a case or make an arrest. This is because NYPD has also left the District Attorney in the dark about surveillance technology. This lack of transparency by NYPD will make it difficult for prosecutors to comply with the new discovery statutes, and as a result could undermine the very intent of discovery reform and clog up the court system in the process.

IV. Police Accountability and Body Cameras

Body worn cameras, if utilized properly, can help to shed light on the thousands of law enforcement interactions many New Yorkers, particularly Black and Latinx people, experience each day. Police misconduct continues to go unmonitored and unchecked and the secrecy of police disciplinary systems perpetuates this misconduct and precludes public scrutiny of law enforcement officers. The ability to capture misconduct with body worn cameras can and should provide judges, prosecutors, and other law enforcement officers with the tools necessary to call

into question officers' credibility, preclude officers from testifying, appropriately dismissing certain cases, and removing officers from the force.

The use of body worn cameras, according to Mayor Bill de Blasio, can deliver "the transparency and policing reforms at the center of effective and trusted law enforcement."[7] It's clear that the use of body worn cameras is significant for transparency. However, members of the NYPD are given full control over when and whether to activate their body-worn cameras, and they have not delivered the transparency that was promised.

Research has shown that officers wearing body cameras were involved in fewer use-of-force incidents and body worn cameras can also increase the likelihood that an officer acting on racial biases [or committing misconduct] will be discovered, investigated, and disciplined. [8] Again, as iterated above, body cameras are only a useful tool to assist in transparency and accountability if they are used properly and judges, prosecutors, and law enforcement officers investigate and carry out disciplinary measures for incidents of misconduct. At the very least, Int. 0487 will answer more questions about the growing use of body cameras, but ultimately the City Council must regulate them if they are to be a meaningful check on police misconduct.

V. Does the NYPD Share Surveillance with ICE?

BDS greatly appreciates the inclusion in Int. 0487 of a provision requiring reporting on the entities that have access to the information and data collected by NYPD surveillance technology, particularly as it relates to federal immigration enforcement. Knowing which surveillance technology is available to the NYPD is especially important in light of recent steps by federal immigration authorities to capitalize on data—including data gathered by state and local governments—to push forward an anti-immigrant agenda. As a City that has been a leader nationally in providing access to counsel and other protections for immigrants in our communities, we must ensure that our resources are not used to deport the very people we seek to protect.

Over the last few months, the U.S. Department of Homeland Security ("DHS") has proposed policy changes that would result in the collection of DNA from New Yorkers who are detained by the government not for the purpose of preventing crime, but rather to aid in deportations. As the federal government expands its bank of data about all New Yorkers, the City must be transparent about what data we share with the federal government.

---

[7] Elena Burger, Thousands of Low-Profile Cases Could Turn on Police Body Camera Footage, (Apr. 19, 2017), https://www.gothamgazette.com/city/6879-thousands-of-low-profile-cases-could-turn-on-police-body-camera-footage (last visited Dec. 18, 2019).

[8] *See* Murphy, Julian R., *Is It Recording? Racial Bias, Police Accountability, and the Body-worn Camera Activation Policies of the Ten Largest U.S. Metropolitan Police Departments in the USA*, 9 Colum. J. Race & L. 141 (2018).

VI. Conclusion

This common-sense legislation will shine a spotlight on practices that warrant public scrutiny and debate. It is simply unfair and undemocratic for law enforcement to have undisclosed access to rapidly evolving technology despite a long, documented history of abusing surveillance capabilities. It is likewise unfair for law enforcement to point blinding klieg lights on the walking paths through public housing while police and prosecutors peer into peoples' private lives with more and more powerful tools in complete darkness. We need not wonder why many in our city describe their communities as open-air prisons, constantly watched and checked through stop & frisk, Broken Windows policing, or mass surveillance. As the federal government debates reforms to its domestic spying program to quell a national uproar, New York City should lead the country into a new era of transparency. For now, our local law enforcement may be spying on us with tools we have never imagined.

Thank you for your consideration of my comments. I respectfully urge the Council to pass Int. 0487.

If you have any question, please feel free to reach out to Jacqueline Caruana at jcaruana@bds.org.

THE LEGAL AID SOCIETY

Justice in Every Borough.

TESTIMONY

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

A Local Law to amend the administrative code of the city of New York, in relation to creating comprehensive reporting and oversight of NYPD surveillance technologies

Proposed Int. No. 0487-2018 (Public Oversight of Surveillance Technology (POST) Act)

The Legal Aid Society
Criminal Defense Practice
49 Thomas Street
New York, NY 10013
By: Jerome D. Greco
(212) 298-3075
JGreco@legal-aid.org

December 18, 2019

Good afternoon. 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 this Committee for the opportunity to provide testimony on Proposed Int. No. 0487-2018.

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 about 300,000 cases 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 examiners, two staff attorneys, and one supervising attorney, with additional hiring planned in the upcoming year. 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.

SUPPORT FOR INT. NO. 0487-2018 (POST Act)

We support the proposed amendments to the Administrative Code of the City of New York and the New York City Charter that would require oversight of the purchase and use of surveillance technologies by the New York City Police Department ("NYPD"). The Legal Aid Society's extensive criminal defense practice and digital forensic abilities puts us in a unique position to understand the urgent necessity of Int. No. 0487-2018.

As the City of New York inches ever closer to a surveillance nightmare, we have an opportunity to take a step back and return some of that power back to the people. The need for

government transparency is never greater than when policing and surveillance technology are at issue. The POST Act is a minimal check on the invasive tools currently shrouded in darkness, the same tools that further sow distrust of the NYPD in already over-policed neighborhoods.

While the NYPD continues to grow its arsenal of powerful surveillance technologies, it eschews the need for rules and regulations controlling and documenting their use. Even when procedures are put into place, they deliberately create overbroad exceptions and there is little oversight ensuring that the rules are carefully followed in the first place. Furthermore, we suspect that there are surveillance tools which the NYPD is actively hiding, preventing any supervision by the traditional means. Courts and legislators cannot act if they do not know they need to act. They cannot uphold the law or represent their constituents if they do not know the existence of the problem. Defense attorneys cannot advocate for their clients when information about the technology used is withheld from them. Secrecy prevents accountability.

Requiring the distribution of publicly reviewed impact and use policies and oversight of compliance with the policies by the NYPD Inspector General will help ensure that the NYPD's procurement and use of surveillance technology is not abused and complies with constitutional and statutory restrictions, while not undermining security.

On behalf of the Legal Aid Society, I testified in 2017 when the POST Act was originally introduced and I stand by my early testimony.[1] While I previously testified about multiple NYPD surveillance tools and we are aware of several other forms of NYPD surveillance,[2] I will restrict this testimony to facial recognition, GPS "pinging", drones, and the Domain Awareness System.

---

[1] *See* Written Testimony of Digital Forensics Staff Attorney Jerome D. Greco, Legal Aid Society, Before the New York City Council Committee on Public Safety in favor of the POST Act, June 15, 2017, https://docdro.id/l0lGL2P [last accessed Dec. 17, 2019]

[2] *See* Ángel Díaz, *New York City Police Department Surveillance Technology*, Brennan Center for Justice [October 4, 2019], available at https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology [last accessed Dec. 17, 2019]

The NYPD's continuous expansion of its surveillance technology makes it impossible to address every tool or issue here.

A. Facial Recognition

In 2017, my POST Act testimony included a substantial section describing the problems with the NYPD's use of facial recognition including race, age, and gender biases, and the lack of scientific reliability. Additionally, I discussed the NYPD's refusal to provide records in regards to its use of facial recognition technology. Unfortunately, there is little to update here because the same problems persist two years later. Georgetown Law's Center on Privacy & Technology's Freedom of Information Law Article 78 against the NYPD is still pending.[3] The NYPD's facial recognition technology remains entrenched in secrecy and its use continues with little guidance.

The Legal Aid Society's Digital Forensics Unit has been able to gather bits and pieces about the NYPD's facial recognition system. This information has been obtained from litigating the use of facial recognition technology in criminal cases across the five boroughs, the Center on Privacy & Technology's lawsuit, and *The Perpetual Line-up*[4] and *Garbage In, Garbage Out*[5] reports. From our understanding, typically, a detective submits a photo to the Facial Identification Section (FIS) to be processed in the facial recognition system. The photo, known as a probe photo, may be a social media photo or a still from video surveillance. The probe photo may be manipulated in multiple ways including editing eyes or a mouth onto it, changing the lighting, mirroring one half of the face to the other half, etc. Once submitted the system returns 200+ possible matches, ranked in order of which arrest photos the system finds are most similar to the probe photo. The same FIS detective then visually compares the 200+ possible matches

---

[3] *Center on Privacy & Technology v. NYPD*, Index #154060-2017 [Sup Ct. N.Y. Co. 2017]
[4] Clare Garvie, Alvaro Bedoya, & Jonathan Frankle, *The Perpetual Line-up: Unregulated Police Face Recognition in America*, Georgetown Law's Center on Privacy & Technology [Oct. 18, 2016], available at https://www.perpetuallineup.org/ [last accessed Dec. 17, 2019]
[5] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Georgetown Law's Center on Privacy & Technology [May 16, 2019], available at https://www.flawedfacedata.com/ [last accessed Dec. 17, 2019]

and makes an "independent" observation of which person he thinks is most likely the person in the probe photo. Other members of FIS are then shown the two photos and verify the "possible match." The FIS detective then sends a "possible match" form to the originating detective that includes the chosen arrest photo and all the pedigree and charge information associated with that arrest.

Though the NYPD agrees that this possible match is not enough by itself for probable cause to make an arrest, there does not appear to be any standard or procedures for what the detective should do next or if the possible match can be used at all in the determination of probable cause. Is the possible match enough to stop someone on the street? Is it enough to pull their car over? Is it enough to appear at their home? Is it enough to place the person in a line-up?

Furthermore, the NYPD has claimed that the database of comparison photos only contains arrest photos from open cases or unsealed convictions.[6] We now know that the NYPD has juvenile arrest photos from children as young as eleven years old in its database,[7] sealed arrest photos,[8] and we suspect that other photos like social media photos are being used as well, despite their claims to the contrary.

Many of the facial recognition abuses and potential abuses can be prevented by giving the NYPD Inspector General authority to monitor and publicly report on the impact and use of this surveillance technology. We should not have to wait years for the possibility that extended litigation or a tip to a media outlet uncovers the misuse of surveillance technology that is occurring now.

---

[6] James O'Neill, *Opinion: How Facial Recognition Makes You Safer*, NY Times, June 9, 2019, available at https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html [last accessed Dec. 17, 2019]

[7] Joseph Goldstein & Ali Watkins, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database*, NY Times, Aug. 1, 2019, available at https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html [last accessed Dec. 17, 2019]

[8] Michael Hayes, *The NYPD is Using Sealed Mugshots in its Facial Recognition Program*, OneZero, Aug. 27, 2019, available at https://onezero.medium.com/exclusive-the-nypd-is-using-sealed-mug-shots-in-its-facial-recognition-program-bd5678ad5632 [last accessed Dec. 17, 2019]

B. GPS Pinging

Prior to the use of cellular phones, the 911 call system could determine a location of a caller based upon the number the person was calling from and the address that number was assigned to. This does not work for cell phones because of their mobility; a person can be calling 911 far from the address connected to their number. In order to remedy this problem, the 911 system is being upgraded to the Enhanced 911 (E-911) system across the country, requiring a caller's cell phone to provide its GPS coordinates to the Public Safety Answering Point (911 operating center).[9] There are additional upgrades expected like text-to-911.[10]

While the E-911 system's attempt to more precisely locate a caller may be seen as an admirable goal, the NYPD is manipulating that system to precisely track the movements of people and rarely obtaining a warrant to do so. This technique is often referred to as "GPS pinging." GPS pinging is an exploitation of the E-911 system which requires the cell phone service provider to send a signal to a cell phone to force the phone to provide its GPS coordinates to the phone company in real-time or near real-time without the customer calling 911 or being aware it is occurring. The coordinates are then provided to the NYPD, typically through an automated system. Pinging is undetectable to the user of the device.

Despite U.S. Supreme Court's ruling in *Carpenter v. United States*,[11] it is rare that we have seen the NYPD or the NYC District Attorney's Offices obtain a warrant prior to using GPS pinging to track an individual. More commonly, they are seeking pen register and trap-and-trace orders from the court pursuant to C.P.L. Article 705, instead of warrants under C.P.L. Articles

---

[9] *Enhanced 911 – Wireless Services*, Federal Communications Commission, available at https://www.fcc.gov/general/enhanced-9-1-1-wireless-services [last accessed Dec. 17, 2019]

[10] *Text to 911: What You Need to Know, Federal Communications Commission*, available at https://www.fcc.gov/consumers/guides/what-you-need-know-about-text-911 [last accessed Dec. 17, 2019] and Reuven Blau, *Long-Promised Power to Text 911 Still Hasn't Arrived on the Scene*, The City, Sept. 16, 2019 , available at https://thecity.nyc/2019/09/long-promised-911-texting-still-hasnt-arrived-on-the-scene.html [last accessed Dec. 17, 2019]

[11] 138 S.Ct. 2206 [2018] (requiring a warrant for the government to obtain seven or more days of historical cell-site location information from a third-party phone company)

690 and 700. Put simply, the NYPD is misleading the courts. GPS pinging is not a pen register and works much differently than a pen register or a trap-and-trace device. As the Supreme Court identified in *Carpenter*, cell phone location information has a reasonable expectation of privacy, unlike the identification and logging of outgoing numbers dialed and the origination of numbers of incoming calls,[12] which are the sole capabilities of pen registers and trap-and-trace devices. Moreover, an order for a pen register requires only reasonable suspicion and not a warrant pursuant to probable cause.[13] It also has less conditions and requirements before it can be obtained.[14]

In *People v. McDuffie*,[15] the NYPD pinged the defendant's phone 3,275 times over two weeks, including sixty times alone on the day of his arrest. This means that the NYPD obtained the precise GPS location of the defendant's phone over 3,000 times in fourteen days with a pen register order, not a warrant. While the *McDuffie* Court found that there was probable cause in the pen register order, it ordered a hearing "[b]ecause the People have not adequately explained the extent and result of the pinging" and the "picture of a prolonged effort over two weeks with over 3000 attempts made to contact and locate defendant's mobile phone is much different than the impression created of a few lucky pings pinpointing a location that confirmed other evidence."[16]

The NYPD has deployed multiple methods to track people by the use of their cell phones without warrants. The use of pen register orders, instead of warrants, is a façade to hide their real requests from the courts. If they truly had probable cause and did not intend to deceive then they would have obtained warrants, which would have more clearly defined their actual intentions.

---

[12] *See Smith v. Maryland*, 442 U.S. 735 [1979] (the installation and use of a pen register does not require a search warrant)
[13] C.P.L. §705.10(2) compared with §690.10 and §700.15(2)
[14] C.P.L. §705.10(2) compared with §700.15(2-5)
[15] *People v. McDuffie*, 58 Misc.3d 524 [Sup Ct. Kings Co. 2017]
[16] *Id.* at 533.

C. Drones[17]

On December 4, 2018, the NYPD announced it possessed fourteen drones.[18] It is unclear where the funding for the drones came from, who the NYPD contracted with to purchase them, and whether they had previously used or possessed drones prior to the fourteen described. With the announcement of their new technology, the NYPD attempted to placate any critics by also publishing a new policy to govern their use of the drones, Interim Order #101 of 2018, which later became an official part of the Patrol Guide, Section 212-124. It bears noting that the NYPD can change the Patrol Guide at any time, since it is not a binding statute.

From a quick glance the Patrol Guide's regulation of drones appears to provide a consistent procedure with necessary restrictions but a closer look reveals two significant problems. First, the limits on the circumstances in which a drone can be used are invalidated by the addition of "A UAS may be used for the following purposes…**or other situation with the approval of the Chief of Department**." (emphasis supplied). This exception opens the use of a drone for any reason approved by the Chief of Department, despite any other constraints listed. Second, while the Patrol Guide explicitly prohibits footage obtained by a drone being subject to facial recognition analysis, there is again a vague exception that negates the restriction: "UAS footage will not be subject to facial recognition analysis, **absent a public safety concern**." (emphasis supplied). A public safety concern is never defined nor does it state who will determine when something is a public safety concern.

In less than a year, we have seen the NYPD uses drones at the Pride March[19] and the Puerto Rican Day Parade.[20] They have also used drones at the Women's March, St. Patrick's

---

[17] The NYPD refers to a drone as an Unmanned Aircraft System (UAS) or an Unmanned Aerial Vehicle (UAV)
[18] *NYPD Unveils New Unmanned Aircraft System Program*, The Official Website of the City of NY, Dec. 4, 2018, available at https://www1.nyc.gov/site/nypd/news/p1204a/nypd-new-unmanned-aircraft-system-program/ [last accessed Dec. 17, 2019]
[19] PD 620-151 Unmanned Aircraft System (UAS) Deployment Report for June 30, 2019, available at https://docdro.id/10qjsk0 [last accessed Dec. 17, 2019]

Day Parade, and New Year's Eve.[21] Though these events would seem to have similar issues and concerns, the documented reasons for the use of drones at these events vary,[22] seemingly indicating that either the justifications are not legitimate or that the officers have little guidance on which reason is appropriate for the events.

Furthermore, an attempt at clarifying the reason for the use of drones at the Pride March through a Freedom of Information Law (FOIL) request was denied.[23] According to the Patrol Guide, the NYPD retains drone footage for thirty days. My FOIL request was made within the retention period but denied because the NYPD had allowed the video to be deleted. The FOIL Officer claimed that since "no UAS video had ever been requested before, the retention policy was unknown to this office at the time of your request."[24] The FOIL Office is bound by the Patrol Guide and therefore was required to be familiar with the drone video retention policy.

D. Domain Awareness System

The NYPD has a vast network of internal databases and records, as well as access to numerous external databases. The public's awareness of the potential harm caused by collection, use, and manipulation of data is increasing as reports of leaks and U.S. Congressional hearings for the largest tech companies in the world become a regular occurrence. The NYPD's growing reliance on data also needs to be subject to oversight to prevent misuse, inaccuracies, and inadequate privacy and security measures. The longer we wait the more difficult it becomes to address the problems and the more people that are harmed in the meantime.

---

[20] PD 620-151 Unmanned Aircraft System (UAS) Deployment Report for June 9, 2019, available at https://docdro.id/sed2rWP [last accessed Dec. 17, 2019]
[21] Mark Chiusano, *First NYPD drone flights, as per deployment records*, AM NY, July 23, 2019, available at https://www.amny.com/mark-chiusano/nypd-drones-records-deployments-1.34206008/ [last accessed Dec. 17, 2019]
[22] *Id.*
[23] Freedom of Information Law Request: FOIL-2019-056-11838.
[24] *Id.*

Again, it is not possible to discuss all of the NYPD databases because they are numerous and likely there are ones we do not even know about. Here, I will briefly mention the Domain Awareness System.

In approximately 2013, the NYPD described the Domain Awareness System (DAS) as

> …a central platform used to aggregate data from internal and external closed-circuit television cameras (CCTV), license plate readers (LPRs), and environmental sensors, as well as 911 calls and other NYPD databases. The DAS uses an interactive dashboard interface to display real-time alerts whenever a 911 call is received or a sensor is triggered. The DAS also includes mapping features that make it possible to survey and track targets.[25]

The Domain Awareness System continues to grow, in both the quantity of data and type of data but its Public Security Privacy Guidelines[26] have not been updated since they were issued in April 2009.

DAS includes data from approximately 500 automated license plate readers with a continuous stream of additional license plate scans and also data from over 6,000 cameras around the City.[27] Additionally, any NYPD officer can access the vast surveillance technology of DAS through an NYPD issued smartphone.[28] The 2009 Privacy Guidelines did not take into account the addition of video analytics to DAS nor has there been any other publicly released information that regulates it. One variation of such video analytics was the NYPD's collaboration with IBM that automatically "tagged" objects and people in video, including

---

[25] *Developing the NYPD's Information Technology*, Official Website of the City of NY, available at http://home.nyc.gov/html/nypd/html/home/POA/pdf/Technology.pdf [last accessed Dec. 17, 2019]
[26] *Public Security Privacy Guidelines*, Official Website of the City of NY, April 2, 2009, available at http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf [last accessed Dec. 17, 2019]
[27] *See* Testimony of Deputy Commissioner of Intelligence and Counterterrorism John J. Miller, New York City Policy Department, Before the New York City Council Committee on Public Safety in opposition to the POST Act, June 15, 2017, at 22-23.
[28] E. S. Levine, Jessica Tisch, Anthony Tasso, Michael Joy (2017) The New York City Police Department's Domain Awareness System. Interfaces 47(1):70-84. https://doi.org/10.1287/inte.2016.0860

identifying people by skin color.[29] Considering the history of the NYPD's racially biased policing, a system that can automatically identify an individual's skin color lends itself to be abused. Even more concerning is that an inaccurate determination or identification can lead to a false arrest or harassment of an innocent person.

Moreover, the NYPD and Microsoft have sold the Domain Awareness System to other police agencies with the NYPD receiving a thirty percent cut of the revenue for each sale.[30] It is unclear how these funds are accounted for, how they are used, and if there is any oversight of this money.

E. We Cannot Rely on the NYPD to Police Itself

The NYPD has repeatedly shown that it cannot be trusted to oversee its own use of surveillance, technology, or biometrics. For example, in violation of the New York Family Court Act, the NYPD had been retaining the fingerprints of juveniles for years.[31] It was only by the work of the Legal Aid Society's Juvenile Rights Practice that this unlawful procedure was discovered and stopped. The violations themselves were significant and the NYPD's attempts to prevent the truth from being uncovered exacerbated the problem. It was only after months of persistent work, by the Legal Aid Society's Christine Bella and Lisa Freeman, and the production of records from New York State's Division of Criminal Justice Services that the NYPD finally conceded its misconduct and agreed to change.[32] Transparency was the tool for change there but it should never have been that difficult. If any of the circumstances had been different the NYPD would still be unlawfully retaining juvenile fingerprints.

---

[29] George Joseph & Kenneth Lipp, *IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color*, The Intercept, Sep. 6, 2018, available at https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/ [last accessed Dec. 17, 2019]

[30] E. S. Levine, Jessica Tisch, Anthony Tasso, Michael Joy (2017) The New York City Police Department's Domain Awareness System. Interfaces 47(1):70-84. https://doi.org/10.1287/inte.2016.0860

[31] Alice Speri, *The NYPD Kept an Illegal Database of Juvenile Fingerprints for Years*, The Intercept, Nov. 13, 2019, available at https://theintercept.com/2019/11/13/nypd-juvenile-illegal-fingerprint-database/ [last accessed Dec. 17, 2019]

[32] *Id.*

In fact, the NYPD continues to skirt the law in its DNA collection practices. Even though New York law requires a warrant or court order for a DNA sample,[33] police officers routinely collect DNA surreptitiously from people in custody.[34] Video footage reported in the media showed police tricking a man into giving DNA by handing him a cigarette.[35] The New York Times confirmed that this kind of DNA collection occurs with children as young as 12.[36] And in Howard Beach, police used coercive tactics to collect DNA from more than 360 men of color,[37] reportedly targeted because of their race.[38] Once the NYPD collects this DNA, it is stored in an unregulated City index that it is difficult, if not impossible, to get out of.[39]

The POST Act will provide the essential transparency and accountability mechanisms to help prevent any ongoing or future abuses of surveillance technology.

CONCLUSION

It is necessary to pass the POST Act to ensure the rights of the citizens of New York City are not violated while still balancing the need for the NYPD to provide effective law enforcement. The Legal Aid Society supports the proposed bill and encourages the City Council to pass it.

---

[33] *Samy F. v. Fabrizio,* 176 A.D.3d 44, 53 [1st Dept. 2019] ("After an arrest, but preconviction, a DNA sample may only be obtained from a suspect on consent, or by warrant or court order.")

[34] George Joseph, *How Juveniles Get Caught Up In The NYPD's Vast DNA Dragnet*, Gothamist, Jan. 10, 2019, available at https://gothamist.com/news/how-juveniles-get-caught-up-in-the-nypds-vast-dna-dragnet [last accessed Dec. 17, 2019]

[35] *Id.*

[36] Jan Ransom & Ashley Southall, *N.Y.P.D. Detectives Gave a Boy, 12, a Soda. He Landed in a DNA Database*, NY Times, Aug. 15, 2019, available at https://www.nytimes.com/2019/08/15/nyregion/nypd-dna-database.html [last accessed Dec. 17, 2019]

[37] Graham Rayman, *NYPD detectives demanded DNA swabs from hundreds of black and Latino men while hunting killer of Howard Beach jogger*, NY Daily News, May 10, 2019, available at http://www.nydailynews.com/new-york/nyc-crime/ny-men-caught-up-in-nypd-jogger-dna-dragnet-object-to-the-tactic-20190510-h4i4q7p4wzhtbpmjmdilvxsc5u-story.html [last accessed Dec. 17, 2019]

[38] Jan Ransom & Ashley Southall *'Race-Biased Dragnet': DNA From 360 Black Men Was Collected to Solve Vetrano Murder, Defense Lawyers Say*, NY Times, Mar. 31, 2019, available at https://www.nytimes.com/2019/03/31/nyregion/karina-vetrano-trial.html [last accessed Dec. 17, 2019]

[39] Aaron Morrison, *Hundreds of Victim and Witness DNA Profiles Removed from New York City Database*, The Appeal, Nov. 26, 2019, available at https://theappeal.org/new-york-dna-database-victims-witnesses-removed/ [last accessed Dec. 17, 2019]

New York Office
40 Rector Street, 5th Floor
New York, NY 10006-1738

T 212.965.2200
F 212.226.7592

www.naacpldf.org

LDF
DEFEND EDUCATE EMPOWER

Washington, D.C. Office
700 14th Street, NW, Suite 600
Washington, D.C. 20005

T 202.682.1300
F 202.682.1312

Testimony of the NAACP Legal Defense and Educational Fund, Inc.

New York City Council's Committee on Public Safety

In Support of Int. No 187 – Creating Comprehensive Reporting and Oversight of NYPD Surveillance Technologies

December 18, 2019

Chairperson Richards and Councilmembers:

My name is John Cusick, and I am a Litigation Fellow at the NAACP Legal Defense and Educational Fund, Inc. ("LDF").

I. Introduction

On behalf of LDF, we thank the Committee on Public Safety for holding this critical hearing on the Public Oversight of Surveillance Technology ("POST") Act – Int. No. 0487-2018, which would create comprehensive reporting and oversight of the New York City Police Department's ("NYPD") surveillance technologies.

LDF is the nation's first and foremost civil and human rights law organization. Since its founding nearly eighty years ago, LDF has worked at the national, state, and local levels to pursue racial justice and eliminate structural barriers for African Americans in the areas of criminal justice, economic justice, education, and political participation.[1] As part of this work, LDF has also forged longstanding partnerships with local advocates, activists, and attorneys to challenge and reform unlawful and discriminatory policing in New York City, including serving as co-counsel in *Davis v. City of New York*, a federal class-action lawsuit that challenged the New York City Police Department's ("NYPD") policy and practice of unlawfully stopping and arresting New York City Housing Authority ("NYCHA") residents and their visitors for trespassing without the requisite level of suspicion.[2]

For reasons described in more detail below, LDF is deeply concerned about the NYPD's surveillance technology, especially tools that use artificial intelligence or an automated decision system ("ADS"),[3] without public engagement, transparency, or oversight. The NYPD's use of these tools threatens to exacerbate racial inequities in New York City. The potential discriminatory effect of these systems on New York City's Black and Latinx residents raises concerns similar to the racially discriminatory and unconstitutional policing practices that historically motivated—and continue to motivate—LDF's litigation, policy, and public education advocacy.

To address these concerns, the New York City Council must ensure that the NYPD's surveillance technology tools are unbiased, transparent, and rigorously

---

1 *About Us*, LDF (2019), https://www.naacpldf.org/about-us/.

2 *Davis v. City of New York*, LDF (2019), https://www.naacpldf.org/case-issue/davis-v-city-new-york/.

3 For this testimony, automated decision system is defined as "any software, system, or process that aims to automate, aid, or replace human decision-making. Automated decision systems can include both tools that analyze datasets to generate scores, predictions, classifications, or some recommended action(s) that are used by agencies to make decisions that impact human welfare, and the set of processes involved in implementing those tools." Rashida Richardson, ed., *Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force*, AI Now Institute 1, 20 (Dec. 4, 2019), https:// ainowinstitute.org/ads-shadowreport-2019.html.

evaluated. Critically, these tools must not undermine the City's commitment to public safety practices that are constitutional and non-discriminatory. Equally important, the process for this accountability and transparency must center on communities that are directly impacted by these tools. LDF, therefore, urges each New York City Council member to support the passage of the POST Act.

II. The Harms Stemming from the NYPD's Surveillance Technology Tools

The NYPD's surveillance technology poses significant risks to racial equality, privacy, public health, civil liberties, and civil rights. New Yorkers know all too well how these tools have been used by the NYPD to profile, target, and punish our communities, especially communities of color and certain religious and immigrant communities. In 2017, it was reported that the NYPD secretly spied on lawful Black Lives Matter protesters by monitoring their cell phones and social media.[4] The NYPD was sued for its practice of illegal spying and blanket surveillance of Muslim New Yorkers.[5] Indeed, the academic walls of John Jay College did not prevent the NYPD from running surveillance operations of the Muslim Students Association, of which I was a member.[6] And, as detailed above, the NYPD relies on a secretive gang database to surveil and execute military-style gang "takedowns" that target boys and young men of color in low-income communities and public housing complexes.[7] These few examples reveal how these new tools can be a part of the abusive surveillance technology being used by law enforcement against vulnerable communities, both locally and nationally.

The NYPD's increasing reliance on surveillance technology tools which use an ADS—such as social-media mining, facial recognition, and predictive modeling—creates an unprecedented and potentially limitless expansion of police surveillance.[8] Of

---

4 Max Jaeger, *Emails Reveal How NYPD Secretly Kept Tabs on Black Lives Matters Activists*, N.Y. Post (Jan. 17, 2019), https://nypost.com/2019/01/17/emails-reveal-how-nypd-secretly-kept-tabs-on-black-lives-matter-activists/.

5 Matt Apuzzo and Adam Goldman, *After Spying on Muslims, New York Police Agree to Greater Oversight*, N.Y. Times (Mar. 6, 2017), https://www.nytimes.com/2017/03/06/nyregion/nypd-spying-muslims-surveillance-lawsuit.html; *An Investigation of NYPD's Compliance with Rules Governing Investigations of Political Activity*, N.Y.C. Dept. of Investigation and Office of the Inspector General for the NYPD, 1, 1 (Aug. 2016), https://www1.nyc.gov/assets/oignypd/downloads/pdf/oig_intel_report_823_final_for_release.pdf.

6 Andre Tartar, *John Jay College President Calls Out NYPD for Spying on Muslim Students*, New Yorker (Oct. 27, 2012), https://nymag.com/intelligencer/2012/10/john-jay-president-calls-out-nypd-for-spying.html; Chris Hawley, *NYPD Monitored Muslim Students All Over Northeast*, Associated Press (Feb. 18, 2012), https://www.ap.org/ap-in-the-news/2012/nypd-monitored-muslim-students-all-over-northeast.

7 Ben Hattem, How Massive Gang Sweeps Make Growing Up in the Projects a Crime, GOTHAMIST (Oct. 24, 2016, 11:02 AM), http://gothamist.com/2016/10/24/gang_sweeps_public_housing.php#photo-1.

8 Ángel Diaz, *New York City Police Department Surveillance Technology*, Brennan Center for Justice at NYU School of Law (Oct. 4, 2019), https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology ("Brennan Center Report"); *Automated Decision Systems: Examples of Government Use Cases*, AI Now (Apr. 11, 2019),

equal concern is the risk that these tools will cast an undue level of suspicion on communities, especially communities of color, that have already suffered from racially biased policing.

Predictive policing tools, for example, threaten to exacerbate the existing racial inequities in policing. Because algorithms learn and transform through exposure to data, an algorithm is only as good as the data that informs it. An ADS's algorithm, therefore, will replicate any biases within its training data—a phenomenon called "training bias."[9] In other words, bias in, bias out. In the policing context, this means that data derived from and reflecting any of the NYPD's practices that are discriminatory, illegal, and unconstitutional will infect any algorithm and any ADS that is trained with that data. The resulting data-driven outcome will then carry out and perpetuate that same discrimination, making all decisions either produced by the ADS or on based on ADS-generated predictions inherently flawed.

Based on the well-documented and judicially recognized history of the NYPD's unconstitutional and racially discriminatory policing practices, we have substantial concerns that the NYPD's datasets are infected with deeply rooted, anti-Black prejudices and other biases.[10] Any predictions or output from a surveillance tool that relies on such data, in any capacity, will reproduce and reinforce this anti-Black prejudice and other biases.

These tools further threaten to redefine the public sphere. The use of predictive modeling, especially when combined with increased surveillance through social media monitoring and facial recognition, may curtail people's freedom of association and speech. If association with friends and family members, or hanging out in what have been labeled "chronic crime" neighborhoods, is used as a factor to justify law enforcement contact and surveillance, many people will be forced to unnecessarily change their lives or risk being subjected to unwarranted police intrusion. And, of course, many others do not have the capability or opportunity to adapt their lives to avoid these risks.

---

https://ainowinstitute.org/nycadschart.pdf.

9 Solon Barocas and Andrew Selbst, Big Data's Disparate Impact, 104 Cal. L. R. 671, 680-81 (2016).

10 Floyd v. City of New York, 959 F.Supp.2d 540, 660-665 (S.D.N.Y. 2013); *Complaint*, Davis v. City of New York, 2010 WL 9937605 (S.D.N.Y. 2011) (No. 1), https://dev.naacpldf.org/wp-content/uploads/Complaint1.pdf?_ga=2.49083558.141431006.1559743995-2134253651.1504725451; *see also* George Joseph, *NYPD Commander's Text Messages Show How The Quota System Persists*, The Appeal (Dec. 12, 2018), https://theappeal.org/nypd-commanders-text-messages-show-how-the-quotasystem-persists/; Jake Nevins, *'We Didn't Ask Permission': Behind an Explosive NYPD Documentary*, The Guardian (Aug. 23, 2018); https://www.theguardian.com/film/2018/aug/23/nypd-documentarycrime-and-punishment-stephen-maing; Rocco Parascandola and Thomas Tracy, *NYPD Demands All Uniform Officers Undergo 'No Quota' Training for Arrests, Tickets*, N.Y. Daily News (Feb. 15, 2018), https://www.nydailynews.com/new-york/nypd-demands-uniformed-officers-undergo-no-quotatraining-article-1.3823160.

There is also the substantial risk that the NYPD may share aggregated data or surveillance-generated labels, infected by racial and other biases, with other agencies.[11] Last year, members of this Committee, along with then-NYPD Chief of Detectives and now Police Commissioner Dermot Shea, acknowledged that the mere fact someone wears a blue hat and is standing outside of a bodega can lead to a designation as a gang or crew member.[12] These deeply flawed designations, which are relied, at least in part, on racial criteria, could easily be shared with federal authorities. This prospect is particularly alarming given the Trump Administration's widely criticized policies on immigration [13] and treatment of Muslims.[14]

Despite these and many other concerns, the NYPD plans to continue embedding ADS in their surveillance tools at an aggressive pace. For example, at a public event at NYU School of Law on April 3, 2019, the NYPD's Deputy Chief of Policy and Programs, Thomas Taffe, explained that the Department has hired more than 100 civilian analysts since 2017 to use ADS software to analyze the NYPD's crime data.[15] Moreover, based on information and belief, the NYPD has and may continue to be building its own ADS-based surveillance tools.[16] The NYPD is thus poised to continue expanding its capacity to rapidly scale up its use of ADS-based surveillance tools without public accountability and oversight.

Without meaningful community accountability and a comprehensive examination of the full impact of these tools before implementation, the likely harms are imminent, potentially irreversible, and growing exponentially each day. Moreover, these tools are being implemented without regard for the widely known societal and structural inequities that persist in nearly every area of life in our city. New York City's communities of color and other vulnerable communities will disproportionately bear these burdens and harms. This reality should be unacceptable to the City Council given the substantial risks to the residents you represent.

---

11 https://www.nydailynews.com/new-york/nypd-track-fugitives-drive-license-plate-readers-article-1.2133879.

12 Rocco Parascandola, *NYPD Will be Able to Track Fugitives Who Drive Past License Plate Readers Across the U.S.*, N.Y. Daily News (Mar. 2, 2015), https://www.nydailynews.com/new-york/nypd-track-fugitives-drive-license-plate-readers-article-1.2133879.

13 Nereida Moreno, *Chicago Settles Suit with Immigrant Falsely Accused of Gang Ties*, Chi. Tribune (Dec. 7, 2018), https://www.chicagotribune.com/news/ct-met-immigration-lawsuit-settled-1206-story.html.

14 Brian Klass, *A Short History of President Trump's Anti-Muslim Bigotry*, Wash. Post (Mar. 15, 2019), https://www.washingtonpost.com/opinions/2019/03/15/short-history-president-trumps-anti-muslim-bigotry/.

15 See Zolan Kanno-Youngs, *NYPD Number-Crunchers Fight Crime with Spreadsheets*, Wall Street Journal (July 23, 2018), https://www.wsj.com/articles/nypd-number-crunchers-fightcrime-with-spreadsheets-1532381806.

16 Brennan Center Report, *supra* note 8.

III. The NYPD's Systemic Failures with Transparency and Accountability

More than three years ago, in front of this very Committee in a hearing regarding a previous iteration of the POST Act, the NYPD claimed it was the most transparent police department in the world.[17] That claim now, as it did then, stands in stark contrast to the NYPD's actions.

The NYPD, for example, continues to profile, surveil, and catalog mostly young men of color through its secretive and subjective gang enforcement practices. The NYPD maintains a gang database (or "criminal group database") that indiscriminately designated thousands of New Yorkers as members of gangs or local street crews; confers such affiliations disproportionately on Black and Latinx New Yorkers; and fails to provide transparency and due process protections to individuals included in the database. In August of 2018, LDF and the Center for Constitutional Rights sued the NYPD for information that was improperly withheld under New York Freedom of Information Law ("FOIL").[18] We ultimately prevailed in obtaining the requested information, which, in turn, confirmed the extent to which the gang database remains a closely guarded secret from the public. Responses to our information requests, however, should not have required the extensive monetary and time resources expended, including months of negotiations and the filing of an administrative appeal followed by a lawsuit.[19] It should, therefore, come as no surprise that the NYPD received an overall "F" from the New York City Public Advocate's Office for its lack of transparency and responsiveness to FOIL requests.[20] We experienced the NYPD's deliberate failures to provide basic information firsthand.

---

17 C.J. Ciaramella, *NYPD Claims It's the Most Transparent Police Department in the World*, Reason (June 14, 2017), https://reason.com/2017/06/14/nypd-claims-its-the-most-transparent-pol/; *see also* Ali Watson, *NYPD Attempts to Block Surveillance Transparency Law with Misinformation*, The Intercept (July 7, 2017), https://theintercept.com/2017/07/07/nypd-surveillance-post-act-lies-misinformation-transparency/.

18 Civil Rights Groups Sue NYPD Over Failure to Disclose Information on Gang Policing Policies, LDF (Aug. 8, 2018), https://www.naacpldf.org/press-release/civil-rights-groups-sue-nypd-failure-disclose-information-gang-policing-policies/.

19 *See also NYPD Predictive Policing Documents*, Brennan Center for Justice at NYU School of Law, July 12, 2019), https://www.brennancenter.org/our-work/research-reports/nypd-predictive-policing-documents.

20 As Public Advocate, now-Mayor Bill de Blasio issued a scathing report criticizing, in part, the NYPD's lack of transparency and responsiveness under FOIL. The report gave the NYPD an overall grade of "F" for its responsiveness to FOIL Requests. According to the report, nearly one-third of all requests never received a response while 28% of answered requests took more than 60 days to process. Breaking Through Bureaucracy: Evaluating Government Responsiveness to Information Requests in New York City, Off. of Pub. Advoc. for the City of New York 14, 26 (April 2013), http://archive.advocate.nyc.gov//foil/report; *see also FOIL Evasion: The NYPD Sidesteps a Crystal Clear Transparency Statue*, N.Y. Daily News (Oct. 14, 2019), https://www.nydailynews.com/opinion/ny-edit-data-20191014-rzahk2esjjazvdvwb5gnxtsble-story.html.

In addition to its discriminatory practices and noncompliance with its FOIL obligations, the NYPD also evades public scrutiny of its surveillance tools by circumventing public reporting regarding its procurement processes. As this Committee knows, a City agency seeking to purchase a good or service must do so through the local procurement process, which includes public notification and oversight approval from the Mayor's Office, New York City Law Department, City Comptroller's Office, and other agencies.[21] To avoid these reporting requirements, the NYPD utilizes a number of mechanisms to avoid public scrutiny and oversight. For example, NYPD can assert that contracts need to be reviewed in confidence and withheld from public disclosure.[22] The Law Department can also unilaterally declare a contract to be "registered," which relieves the NYPD's of its obligation to have it reviewed by the Comptroller's Office.[23] As another option, the NYPD can sign a nondisclosure agreement with a vendor that may justify withholding information about the surveillance technology.[24] Last, the NYPD can gain access to equipment and technology through the New York City Police Foundation ("Foundation"). The Foundation is not subject to the City procurement processes, meaning that the necessary public notifications and approval process are not in place to ensure transparency and oversight before it purchases certain surveillance technology for the NYPD to deploy.[25] The NYPD's utilization of these methods of procurement forecloses public accountability and transparency about its surveillance technology.

Unfortunately, this veil of secrecy is the norm, not the exception, for the NYPD. Indeed, a litany of recent examples further illustrate the NYPD's systemic failures with transparency. First, the NYPD has been using a software called Patternizr, which allows officers to search through thousands of case files to look for patterns or similar crimes.[26] Despite being in use since 2016, the NYPD disclosed information about Patternizir for the first time in a published journal this year. Second, since at least 2017, the NYPD relies on a facial recognition system during investigations.[27]

---

[21] *About Procurement*, NYC Mayor's Office of Contract Services (2019), https://www1.nyc.gov/site/mocs/about/procurement.page.

[22] Winston, *supra* note 17.

[23] *Id.*; *see also Contract Registration*, New York City Comptroller's Office (2019), https://comptroller.nyc.gov/services/for-city-agencies/contract-registration/; *New York City Spending by Active Expense Contracts*, New York City Comptroller's Office (2019), https://www.checkbooknyc.com/contracts_landing/status/A/yeartype/B/year/120.

[24] *Id.*

[25] Laura Nahmias, *Police Foundation Remains a Blind Spot in NYPD Contracting Process, Critics Say*, Politico (July 13, 2017), https://www.politico.com/states/new-york/city-hall/story/2017/07/13/police-foundation-remains-a-blind-spot-in-nypd-contracting-process-critics-say-113361; *Private Donors Supply Spy Gear to Cops*, Pro Publica (Oct. 13, 2014), https://www.propublica.org/article/private-donors-supply-spy-gear-to-cops.

[26] Andrew Liptak, *The NYPD is Using a New Pattern Recognition System to Help Solve Crimes*, The Verge (Mar. 10, 2019), https://www.theverge.com/2019/3/10/18259060/new-york-city-police-department-patternizer-data-analysis-crime.

[27] Clare Garvie, *Garbage In, Garbage Out*, Georgetown Law Center on Privacy & Technology (May 16,

Information about this system and how the NYPD uses and manipulates photos was first revealed this May in a report by Clare Garvie, entitled *Garbage In, Garbage Out: Face Recognition on Flaw Data.*[28] Third, although it was not implemented, IBM had started to develop identification software for the NYPD from 2009 through 2013, which, among other features, would have let officers search camera footage for images by skin tone.[29] Information about this system was publicly revealed for the first time in 2018 due to investigative reporting.[30] Fourth, without *any* community input or engagement, the NYPD revealed its fleet of fourteen (14) unmanned aircraft systems (or "drones") last December.[31] These examples cast further doubt on NYPD's claim that it is providing meaningful—let alone the most—transparency.

Although we have information about some of the NYPD's surveillance tools, the picture is far from complete. Based on information and belief, the NYPD is deploying and internally building new surveillance tools that are shielded from public view and oversight.[32] Moreover, because the NYPD routinely conceals information about these tools, it is difficult to fully understand the scope of the surveillance technology in its arsenal without mandatory public reporting. Even for tools cited in this testimony, we do not know several vital questions, including their full capabilities, the extent of their use, and whether the acquired data and information is shared with other local, state, and federal law enforcement agencies.

Without public disclosure about the details of its surveillance technology, the NYPD avoids public accountability and transparency to the communities it has sworn to protect and serve. Concealing this information thwarts crucial public debate, including the necessary dialogue with affected communities, while further sowing mistrust between the NYPD and community members. This situation is antithetical to the City's commitment to accountability, fairness, and transparency.

IV. The POST Act

Passage of the POST Act is one significant way to begin mitigating these harms and New Yorkers' well-founded fears. The mandatory public reporting provisions are a critical mechanism to ensure New Yorkers have access to basic information about surveillance tools. As demonstrated by the community forum on ADS recently organized by LDF and other organizations, community members want to engage in robust public

---

2019), https://www.flawedfacedata.com/.

28 *Id.*

29 George Joseph and Kenneth Lipp, *IBM Used Surveillance Footage to Develop Technology that Let's Police Search by Skin Color*, The Intercept (Sept. 6, 2019), https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/.

30 *Id.*

31 Ashley Southhall and Ali Winston, *New York Police Say They Will Deploy 14 Drones*, N.Y. Times (Dec. 4, 2018), https://www.nytimes.com/2018/12/04/nyregion/nypd-drones.html.

32 *See generally* Brennan Center Report, *supra* note 8.

dialogue about these tools and how they may impact their lives. Access to this information should not be concealed by the NYPD through manipulation of the procurement process or flagrant violations of FOIL.

Equally important, New Yorkers want to understand the full impact of these tools on their lives. For the reasons described above, many of the known surveillance tools, especially those with an ADS, threaten to exacerbate existing racial inequity in the City. Certain tools, such as predictive policing, could be used to justify disparate treatment of communities of color in terms of how "suspicion" is defined, who is chosen as "targets" for increased enforcement and surveillance, and where these ADS-based surveillance tools are deployed—all raising significant constitutional concerns under the First, Fourth, and Fourteenth Amendments to the U.S. Constitution, as well as applicable state and local laws. New Yorkers must fully understand how these systems will affect communities. The impact study provisions contained in the POST Act are therefore critical to understanding the effect of the use of the tools, particularly whether they have a racially disproportionate impact. Accordingly, it is critical that any impact study must encompass a racial equity impact assessment.[33]

V. Conclusion

The rapid, unchecked deployment of NYPD's surveillance technology without effective mechanisms for public input and oversight is untenable. Moreover, implementing and relying on these tools without understanding their impact, particularly their racial justice impact, will exacerbate the current inequities throughout the City and may lead to illegal discriminatory behavior. Data and technology should not be weaponized by the City against its residents. The City must therefore reaffirm its commitment to accountability, transparency, and unbiased policing by passing the Post Act. Doing so is a critical first step. But it does not address—and more importantly—does not resolve all the concerns we shared above. For these reasons, we look forward to continuing this vital conversation and welcome the opportunity to discuss additional necessary reforms and solutions.

Thank you for your time and consideration. If you have any questions, please do not hesitate to contact us at 212-965-2200.

---

[33] A Racial Equity Impact Assessment (REIA) is a "systematic examination of how different racial and ethnic groups will likely be affected by a proposed action or decision. REIAs are used to minimize unanticipated adverse consequences in a variety of contexts, including the analysis of proposed policies, institutional practices, programs, plans and budgetary decisions. The REIA can be a vital tool for preventing institutional racism and for identifying new options to remedy long-standing inequities." *Racial Equity Impact Assessment*, The Center for Racial Justice Innovation (2019), https://www.raceforward.org/sites/default/files/RacialJusticeImpactAssessment_v5.pdf.

The Bronx Defenders | Redefining public defense

New York City Council
Committee on Public Safety

Re: Int 0487-2018: Creating Comprehensive Reporting and Oversight of NYPD Surveillance Technologies.
December 18, 2019

Written Testimony of The Bronx Defenders
By Alice Fontier, Managing Director, Criminal Defense Practice

Chairman Richards and members of the Committee, my name is Alice Fontier and I am the managing Director of the Criminal Defense Practice at The Bronx Defenders. I thank the Committee for the opportunity to testify.

The Bronx Defenders ("BxD") is a public defender non-profit that is radically transforming how low-income people in the Bronx are represented in the legal system, and, in doing so, is transforming the system itself. Our staff of over 350 includes interdisciplinary teams made up of criminal, civil, immigration, and family defense attorneys, as well as social workers, benefits specialists, legal advocates, parent advocates, investigators, and team administrators, who collaborate to provide holistic advocacy to address the causes and consequences of legal system involvement. Through this integrated team-based structure, we have pioneered a groundbreaking, nationally-recognized model of representation called holistic defense that achieves better outcomes for our clients. Each year, we defend more than 20,000 low-income Bronx residents in criminal, civil, child welfare, and immigration cases, and reach thousands more through our community intake, youth mentoring, and outreach programs. Through impact litigation, policy advocacy, and community organizing, we push for systemic reform at the local, state, and national level. We take what we learn from the clients and communities that we serve and launch innovative initiatives designed to bring about real and lasting change.

I. The Bronx Defenders Supports The POST Act (Intro 0487-2018)

Over the course of a decade, the New York Police Department has adopted surveillance technologies as a central aspect of its policing strategy. The NYPD has unleashed upon ordinary New Yorkers powerful surveillance tools like cell phone location trackers, license plate readers, body-worn cameras, and facial recognition technology. The adoption and use of such technologies have occurred without meaningful oversight, without independent review of their efficacy and impact, and without establishing legal protections to prevent misuse. While these tools give law enforcement power it has never had before, the NYPD has routinely used them

while shrouded in secrecy, depriving citizens of the opportunity to grapple with the threat that these tools present to our privacy and civil rights.

As public defenders on the front lines representing clients, it's not difficult to see how the NYPD's lack of transparency impairs the integrity of the criminal legal system and impedes our ability to fairly defend our clients. If surveillance technologies are utilized without proper oversight and meaningful legal protections, there can be no assurance that the methods used against an accused by the government are truly reliable or proper. The POST Act, which would require the NYPD to evaluate and publish a use policy for surveillance technologies and institute compliance requirement, is a crucial first step that would increase public trust and strengthen the integrity of the criminal legal system.

II. A Dragnet in the Palm of Their Hands: Surveillance and Policing in New York City

Much of what we know about the tools deployed by the NYPD to surveill New Yorkers has come as a result of litigation, or from the tidbits offered by the department in carefully crafted public relations efforts touting its advances in efficiency and technology prowess. The backbone for these arsenal of tools is the NYPD Domain Awareness System (DAS).

According to publicly available information:

> The DAS is a network of sensors, databases, devices, software, and infrastructure that delivers tailored information and analytics to mobile devices and precinct desktops. Originally designed for counterterrorism purposes, the DAS has been modified for general policing and is now deployed across every police precinct in the City and on the smartphone of every officer.
>
> The DAS informs a variety of tactical and strategic decisions that officers make every day. The analytics and operations research methods built into DAS enable better situational awareness by monitoring and issuing alerts on sensor feeds, such as license plate readers and radiation sensors. When an officer responds to a 911 call, the DAS allows that officer to read records that indicate a propensity for violence at that address. Commanding officers use the predictive analytics built into DAS to help make decisions about where to place their patrols.[1]

The NYPD DAS includes:

1. **All NYPD cameras including stationary, dash cam, and body camera** -- according to recent NYPD testimony before the Council, the NYPD is currently storing over 8 million videos captured by body camera alone
2. **License plate readers** - The NYPD reports storing over 2 billion records, and has stated publicly that they can track any license plate historically and in near real time.
3. **Shot spotter**
4. **Real Time Crime Center data, which includes:**

[1] INFORMS. "NYPD Domain Awareness System (DAS)." *INFORMS*, 2016, www.informs.org/Impact/O.R.-Analytics-Success-Stories/NYPD-Domain-Awareness-System-DAS.

a. More than 5 million New York State criminal records, parole and probation files,

b. More than 20 million New York City criminal complaints, arrests, 911/311 calls and summonses spanning five years,

c. More than 31 million national crime records, and

d. More than 33 billion public records.

5. "other databases"

The NYPD DAS is available in real time on every smartphone carried by NYPD officers. What this means is that with any input - name, address, phone number - all of the records and associated information are available to every officer at that moment. Also, the NYPD cellphones and tablets are all biometric. This means that the phone can input a fingerprint, and search the DAS through that means. The DAS is also linked to a facial recognition system, so simply by taking a photograph, an officer can access billions of records in DAS in real time.

We do not know if NYPD officers actually do this. We only know they are technologically capable. This dragnet of instantly available information is the reason that the POST Act is critical. New Yorkers have a right to know the extent of surveillance to which they are subjected on a daily basis.

III. Lack of Transparency Undermines Integrity of The Legal System

The NYPD's pattern and practice of hiding its surveillance technologies used in its investigations and prosecutions does not create a more just legal system. This lack of transparency effectively allows the NYPD to place its own legal judgments ahead of what's normally generated through an open and adversarial judicial process. Accordingly, it promotes an environment where police officers may leave material facts out of reports and misrepresent the real probable cause for locating or identifying a person of interest. More importantly, it undermines the constitutional rights of the accused by depriving them from making informed and specific arguments to challenge whether the surveillance was lawful.

For example, the NYPD had secretly been using cell-site simulators (Stingray) to identify and track New Yorker's cellphones in the course of an investigation, without fully informing the courts or their attorneys. The NYPD sometimes resorted to a tactic called parallel construction to prevent defense counsel and impacted people from learning about the use of the technology. What this means is, for example, although the police track a cell phone location in real time using a stingray, the official police records will refer to a "confidential source" or other information instead of disclosing the use of the technology. It was only after extensive FOIL litigation that the NYPD was forced to disclose its use of Stingray devices to conduct illegal, warrantless searches of people's whereabouts in over a thousand cases over an eight-year period[2]

[2] Emmons, Alex. "New York Police Have Used Stingrays Widely, New Documents Show." *The Intercept*, 11 Feb. 2016, www.theintercept.com/2016/02/11/new-york-police-have-used-stingrays-widely-new-documents-show

Various other surveillance and digital technology systems are actively used by the NYPD, but defense attorney very rarely actually see a reference to them in criminal cases. The prosecution typically does not seek to admit the use of the technology in evidence, and therefore it cannot be challenged. That same secretive process and intentional obfuscation of surveillance activities is now being done to cover up the use of facial recognition technology and other surveillance tactics. Because of the criminal evidentiary rules, these practices cannot effectively be challenged in court. As a result, people's rights are violated and we fall short of the highest demand our rule of law requires when liberty is at stake.

The NYPD has not admitted to using tactics like parallel construction with respect to facial recognition technology, predictive policing, or other digital technologies, but we have every reason to believe they are. For instance, the NYPD says that thousands of matches have been made using facial recognition technology, yet we have only seen a reference to this technology in a handful of cases. Those that we have seen, the NYPD produced the minimum amount of information possible and actively fought to keep anything additional from the court.

IV. Case Examples

The facts of a couple cases that we have seen demonstrate the problems with operating this technology, such as facial recognition methods, in secret.

a. Mr. LR's Case (Facial Recognition)

Our client, LR, was arrested and charged with Robbery in the First Degree. The charge stemmed from an incident in which a person walked in a department store, took socks, and then was alleged to have threatened the store security officer with a knife as he left. Approximately four months after this alleged incident, LR was arrested. When the assigned defense attorney inquired about the delay and the manner in which our client was identified, the prosecutor responded: "facial recognition."

In this case, the police captured a still image from grainy surveillance video and ran that photograph through the facial identification system (FIS). The FIS produced some number of possible matches - the system is programmed to produce up to 200 possible matches. LR was one of those photographs, and was selected by the officer in the FIS unit as the best possible match. The detective working the case then took LR's single photograph from a prior arrest and sent it by text message to the store security officer and asked "is this the guy?". The security officer responded by text message, saying "that's the guy." LR was then arrested on that basis.

In court, the prosecutor argued that none of the other matches were relevant information that should have been disclosed to the defense, and further that any information about the FIS was not relevant because the prosecutor did not plan to introduce it at trial. The prosecutor intended to have the security officer make an in court identification -- meaning point to the man whose picture he had been sent by text, who was sitting next to the defense attorney. The NYPD for its part, filed motions to quash the subpoena for information about the FIS arguing that it was proprietary information and should not be disclosed in court.

Through these means, despite LR knowing that FIS was a direct cause of his arrest, would be deprived of ever challenging that very same evidence. The judge in that case ordered a hearing on these issues. However, rather than litigate these questions, the prosecution offered LR a misdemeanor and time served. The question of the reliability of the FIS match must be questioned at some time. In this case, LR's son was born two hours after the sock thief was in the department store, and LR was there with him. Adding to the issues in this case, LR has a twin brother.

We know that facial recognition technology is widely used by the NYPD - they have a designated unit of officers. We know that facial recognition technology is not perfectly reliable - but we don't know how the NYPD system operates or how unreliable it might be. We also don't know how often and which people are arrested because of this system. The POST Act is one necessary step in answering these questions.

b. Mr. RG's case (Patternizr)

Patternizr has been in use since 2016, but was only recently revealed publicly by the NYPD.[3] This system was built by the NYPD and uses an algorithm to search arrest reports and generate possible patterns in offenses. We do not know how this information is used, or how often. We have never seen a police report that included a statement that Patternizr was used as a source of information.

The facts of one case that I am aware of would indicate that the NYPD is using the system to make arrests. My client, RG, was arrested in the Bronx on allegations that he and two other people arranged to buy a cellphone, but instead stole the phone at gunpoint. One week after being arraigned on the Robbery charge in the Bronx, he was arrested in Manhattan on another Robbery complaint alleging the same set of facts.

The evidence in the case included one detectives report that stated "[Detective] from Manhattan Robbery Squad informs [the Bronx detective] that he has a similar case and is dropping an i-card." RG was then brought to Manhattan and arrested on that i-card. There was no other connection to Manhattan, and no indication in any paperwork that indicated how the Manhattan detective knew about the Bronx case and that it was "similar." Thus, RG suddenly found himself charged with two violent felonies and facing 15 years in prison. Rather than face the risk of trial and and far more time if convicted, RG accepted a plea agreement that would cover both cases.

In this case, the defense attorneys for RG did not have any information on how the police made their determination identifying him as a suspect in the Manhattan case. They could not test whether a thorough and legitimate police investigation was conducted prior to issuing a warrant for the arrest not only because Mr. RG had few options available to him given the open case, but

[3] Liptak, Andrew. "The NYPD Is Using a New Pattern Recognition System to Help Solve Crimes." The Verge, The Verge, 10 Mar. 2019, www.theverge.com/2019/3/10/18259060/new-york-city-police-department-patternizer-data-analysis-crime

also because it was unlikely that the actual methods utilized by the detective may not come to light and properly challenged in court.

V. CONCLUSION

The Bronx Defenders applauds Councilmember Gibson and the other Co-Sponsors of Intro 0847 which would lift the cloak of secrecy from the NYPD's surveillance technology and practices as well as institute sensible measures of oversight and compliance. The POST Act is an important first step to ensuring transparency that would increase public confidence in the NYPD and allow informed public discussion about government surveillance in New York City. It would also add to the integrity of our legal system and result in more fairness to those who are accused of crimes. We urge the City Council to pass this important legislation.

Thank you again for the opportunity to testify.

Statement from Alex S. Vitale

Professor of Sociology, Brooklyn College

Coordinator of the Policing and Social Justice Project

To the New York City Council

Committee on Public Safety

December 18, 2019

Dear Members of the Committee on Public Safety,

The Policing and Social Justice Project at Brooklyn College is here today to support passage of the POST Act. We believe that the NYPD has an obligation to increase transparency around the use of technology. This technology is being used for public purposes and the public has a right to know what technology is in use and what the rules are that govern that use.

We are especially concerned about the NYPD's utilization of new technologies in its efforts to suppress what it calls "criminal groups" or "gangs." Our recent report "Gang Takedowns in the de Blasio Era: The Dangers of Predictive Policing" documents a number of high-tech strategies being used by the NYPD to suppress gang activity. As part of their efforts, they have created a large database of people with very little public transparency about who is on the database, how they end up there, and more importantly, how the database is used. People on the database have no right to know if they are on it, there is no notification process even for juveniles, and no way to appeal one's inclusion. We are also concerned about the fact that over 90% of those on the database are non-white.

Investigations into gang databases elsewhere have uncovered wildly inaccurate information, racial bias and abusive and illegal practices:

- A recent report by the Chicago Office of the Inspector General found that the Chicago Police Department's database was filled with inaccuracies, was shared with immigration

officials, and "potentially undermines public confidence in the Department's legitimacy and effectiveness in the service of its public safety mission."

- An audit of the Cal Gang database by the California State Auditor found wild inaccuracies in the database including the presence of infant children and raised concerns regarding fundamental privacy protections.

- A review of the UK's Gangs Matrix system by Amnesty International found similar privacy issues based on evidence that data was shared with other government agencies affecting people's access to basic government services and employment. Like the NYPD's gang database, the majority of those in the UK's Gangs Matrix were people of color with little or no criminal history.

- In Portland, OR, police decided to end the use of their database in 2017 rather than reveal its inner workings when requested to do so by local journalists.

That is why we have called for an investigation of the database by the NYPD Office of Inspector General to determine if abuses are occurring in New York. Passage of the POST Act would also be a major step forward in enhancing public accountability in the usage of this database.

We are also concerned about the NYPD's usage of social media surveillance tactics. We know that monitoring of social media accounts is common practice. It is also possible that the department is using software to "scrape" social media sites of data in an attempt to identify individuals for possible inclusion in the criminal group database or to construct social networks. Almost all of the young people so targeted are non-white. Because of a lack of transparency, we do not know for if this technology is in use and how it is being utilized.

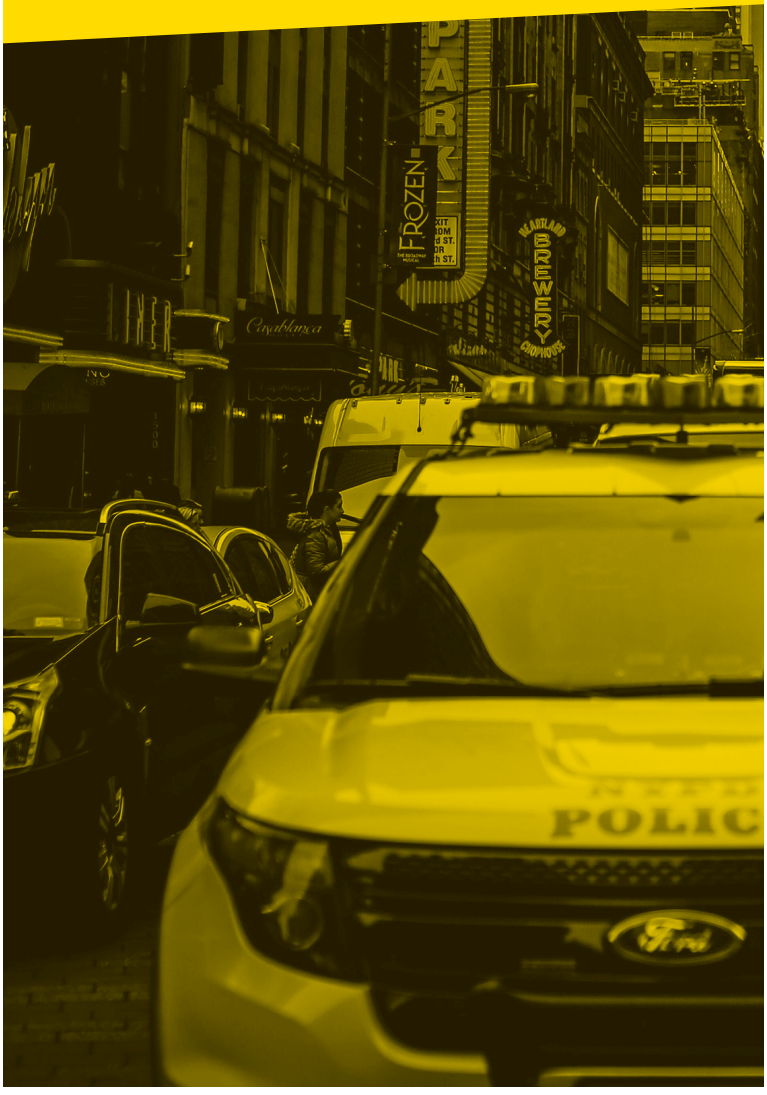
The NYPD may also be using analytic software in its Ceasefire program. That initiative develops lists of youth who are believed to be at high risk for involvement in violence, who are then subjected to intensive threats, surveillance, and harassment. We do not know how these lists are developed. We do know that the Manhattan DA's office has worked with the software company Palantir in the development of its own risk assessment software. A number of objections have been raised about the usage of such analytic software. In New Orleans Palantir had a secret contract with the police department there to produce predictive analytics. Even members of the City Council were unaware of the contract. Palantir has also been criticized for its role in producing "heat lists" for the Chicago Police Department. These lists have historically targeted almost exclusively young people of color and this may be in part because they rely on past involvement with the criminal justice system, which is itself a product of racialize targeting of certain communities for enhanced policing and criminalization.

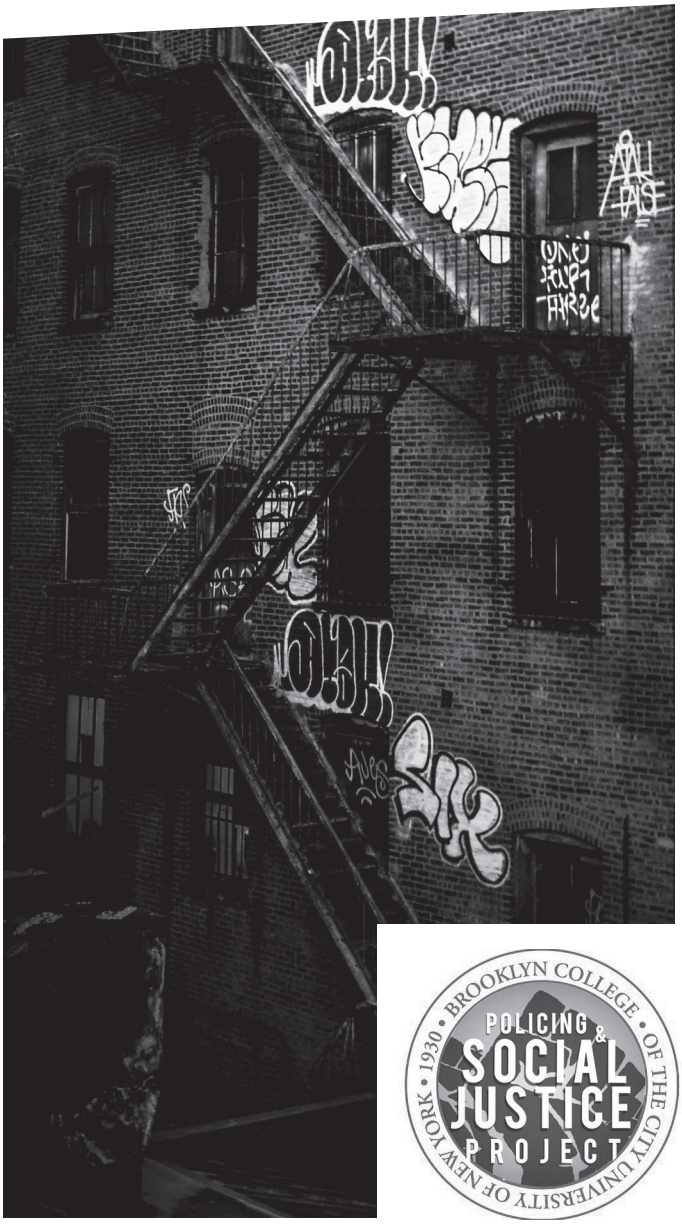
Because of our concerns about the secretive use of technology designed to target almost exclusively people of color, much like "stop, question, and frisk," we urge you to pass the POST Act to enhance public accountability of these police practices.

Thank you.

GANG TAKEDOWNS IN THE DE BLASIO ERA:

The Dangers of ‘Precision Policing’





By JOSMAR TRUJILLO and ALEX S. VITALE

BROOKLYN COLLEGE • 1930 • OF THE CITY UNIVERSITY OF NEW YORK
POLICING & SOCIAL JUSTICE PROJECT

TABLE OF CONTENTS

ABOUT THE POLICING AND SOCIAL JUSTICE PROJECT AT BROOKLYN COLLEGE

The Policing and Social Justice Project at Brooklyn College is an effort of faculty, students and community researchers that offers support in dismantling harmful policing practices. Over the past three years, the Project has helped to support actions, convenings, and community events to drive public education and advocacy against the New York City Police Department's gang policing tactics, including its so-called gang database.

ABOUT THIS REPORT

The compilation of this report includes interviews with people in affected communities and family members as well as survey responses from defense attorneys and insights from advocates. This is not intended to be a quantitative research report. The report is intended to highlight what we know, currently, about gang policing practices in New York City.

This report is limited to policing and, to a lesser extent, prosecution strategies. This report also is limited in its analysis on gangs or gang culture. The expert voices on gangs are those who have lived that reality. We hope this report spurs further research, education and advocacy.

ACKNOWLEDGEMENTS

This report was compiled and edited by Josmar Trujillo and Professor Alex Vitale from The Policing and Social Justice Project at Brooklyn College. Additional research support was provided by Amy Martinez.

Insights from interviews of people directly impacted by gang policing, including public housing residents, inspired and spearheaded this report. In many ways, this report is a reflection of the brave voices of community members and family members including Taylonn Murphy Sr., Darlene Murray, Diane Pippen, Shaniqua Williams, Afrika Owes, Kraig Lewis, mothers from the Bronx120 case, and many more.

The report would not have been possible without the help of **The Bronx Defenders** and **Brooklyn Defender Services** as well as the contributions of **The Legal Aid Society**, specifically Anthony Posada from the **Community Justice Unit** and Michelle McGrath from the **Decarceration Project**. The authors would also like to thank Professor Babe Howell, Vidal Guzman, Nathalia Varela and Judy Greene for their critical feedback.

Many thanks also to the **Vital Projects Fund** for their support.

INTRODUCTION

In 2012, the NYPD initiated a major change in how it deals with issues of youth violence. That year, then Commissioner Ray Kelly announced "Operation Crew Cut," which would double the number of officers in the gang unit from 150 to 300. Kelly made it clear that this new operation was intended to target "loosely affiliated groups of teens" who often "identify themselves by the blocks where they live and are responsible for much of the violence in public housing." [1]

In addition, the NYPD recreated its "Criminal Group Database" to track alleged gang members and wipe out alleged gang violence through large scale conspiracy cases. The result has been thousands of juveniles and adults arrested and charged in gang conspiracy cases, tens of thousands placed into a secretive gang database, and many more subjected to harassment, intimidation, surveillance, and threats.

The new focus on loose associations of young people came just as political and legal challenges to widespread "stop, question, and frisk" practices increased.[2] It appears that the NYPD is merely substituting one set of techniques to tightly manage the lives of young people of color for another and uses the 'gang" label to mute public opposition.[3] The NYPD has taken the term gang and turned it into a marker of violence and lawlessness.

While some people define themselves as gangs, there is nothing illegal about such a grouping in and of itself. Police, however, have chosen to define associations of young people as organized criminal enterprises. And even when such groupings are involved in illegal activity, defining them as "illegal gangs" and attempting to suppress them through mass criminalization is discriminatory and harmful.

Almost every person targeted by these initiatives has been Black or Latinx. This kind of law enforcement relies on the same logic that has driven much of the enormous increase in incarceration over the last 40 years. It is also linked to pathologization of gangs under former mayor Rudy Giuliani at a time when some gangs, namely the Latin Kings, were becoming increasingly politically influential and joining protests against police brutality. The Kings would become the targets of one of the most massive police operations since the era of prohibition.

New York City is making a dangerous and counterproductive mistake in using "gang suppression" techniques to manage the problems of youth violence. Gang suppression policies wrongly assume that deterrence and incapacitation are the only ways to reduce violence. Cities like Oakland, Los Angeles, and Chicago have spent decades trying to "suppress" gangs through intensive surveillance, harassment, and criminalization. These efforts, however, have done nothing to reduce the presence of gangs in these cities. In fact, some research shows that these tactics actually enhance young people's identification with gang life, and makes these gangs more violent. .[4]

When specialized gang units are created they have a tendency to become insulated from oversight from within their departments and from the public. Historically, gang suppression units have been notoriously corrupt and brutal. The LAPD's CRASH Unit, for example, was responsible for widespread human and civil rights abuses and officers in the unit were later found to be dealing drugs, using excessive force, and falsifying arrests. [5]

During the 1960's and 70s, the gang intelligence unit of the Chicago Police Department was directly involved in infiltrating and disrupting the Black Panther Party. They shared information with the FBI's COINTEL Program and coordinated with the State's Attorney Office that orchestrated the assassination of Black Panther leader Fred Hampton. [6]

More recently, officers in Chicago's gang unit were involved in torturing suspects to extract confessions and faking evidence. [7] And just last year an FBI investigation found members of the Area Central gang team were involved in robbing drug dealers. [8]

In Portland, Oregon the local police disbanded their Gang Enforcement Team after an outside review by the Portland City Auditor showed that their proactive enforcement efforts had no positive effect on crime rates, utilized high numbers of improper pretextual traffic stops, and were racially skewed. [9]

The NYPD's own Street Crime Unit, that dealt with "gang crime" at the time, had to be shut down after it was learned that their "We Own the Night" motto reflected their involvement in abuse of force incidents and the killing of unarmed immigrant Amadou Diallo in 1999. The expansion of the size and scope of the New York City's gang units present new risks of corruption and abuse that have been largely ignored by policymakers.

Historically, New York City avoided some of the more severe gang suppression tactics in other cities. In the 1950s and 60s, the City's Youth Board deployed large numbers of street workers to try to connect with young people involved in gangs to try to encourage them to reduce violent conflicts and steer them towards education and employment.[10] By the 1970s, the city established a "Roundtable of Youth" under Mayor Lindsay that met regularly at Gracie Mansion to express youth concerns and attempt to integrate street involved youth into productive problem solving discussions. [11]

As recently as 2008, the Public Advocate's Office recommended that the City "shift resources to alternatives to detention programs... encourage youth programming that meets the specific needs of the community it serves through the Request for Proposals (RFP) process" as well as involving young people directly in anti-violence initiatives.[12] By avoiding strategies that relied primarily on criminalization and avoiding the labeling of youth as gang members, New York did not developed the kind of multi-generational gang violence seen in LA and Chicago.

This report does not attempt to define what a "gang" is or isn't. Gangs are not legally defined in New York state either. This report, produced in collaboration with legal and community groups, seeks to document and provide a primer of what is known about New York City's gang policing infrastructure, including its gang database. Through surveys of defense attorneys and public residents, it highlights the voices of those who see how gang allegations impact people in courtrooms and in their communities.

This report is not intended to be an exhaustive audit of gang policing tactics, which have been developed in secrecy by police. It is intended to be a starting point to encourage more research, transparency and advocacy.

1 Associated Press, "NYPD Plans to Double Size of Gang Unit." USA Today. October 10, 2012. https://www.usatoday.com/story/news/nation/2012/10/02/nypd-gangs-social-media/1607799/
2 K. Babe Howell, "Gang Policing: The Post Stop-and-Frisk Justification for Profile-Based Policing." 5 Univ. Denver Crim. Law Rev. 1. 2015. and Joseph Goldstein & J. David Goodman, Frisking Tactic Yields to Focus on Youth Gangs, New York Times. Sept. 18, 2013, at A1. https://www.nytimes.com/2013/09/19/nyregion/frisking-tactic-yields-to-a-focus-on-youth-gangs.html.
3 Howell, "Gang Policing." and Stephon Johnson, Stop-and-Frisk Makes Way for Operation Crew Cut, Amsterdam News. Sept. 26, 2013, http://amsterdamnews.com/news/2013/sep/26/stop-and-frisk-makes-way-operation-crew-cut/.
4 David C. Brotherton, Youth Street Gangs. New York: Routledge. 2015. Malcolm W. Klein, Gang Cop. New York: AltaMira Press. 2004. Judith Green and Kevin Pranis, "Gang Wars: The Failure of Enforcement Tactics and the Need for Effective Public Safety Strategies." Justice Policy Institute. 2007.
5 Joe Domanick, Blue: The LAPD and the Battle to Redeem American Policing. New York: Simon and Schuster. 2015. Max Felker-Kantor, Policing Los Angeles. Chapel Hill, UNC Press. 2019.
6 Simon Balto, Occupied Territory: Policing Black Chicago from Red Summer to Black Power. Chapel Hill, UNC Press. 2019 p.201-204.
7 Spencer Ackerman and Zach Stafford, "Chicago Police Detained Thousands of Black Americans at Interrogation Facility. The Guardian. Aug 5, 2015. https://www.theguardian.com/us-news/2015/aug/05/homan-square-chicago-thousands-detained
8 Jason Meisner et al, "Chicago Cops Stripped of Powers as FBI probes Ripoffs of Drug Dealers." The Chicago Tribune. Feb 1, 2018. https://www.chicagotribune.com/news/breaking/ct-met-chicago-cops-stripped-fbi-sting-20180131-story.html.
9 Portland City Auditor, "Gang Enforcement Patrol." Portland City Auditor, Audit Services Division. 2017. https://www.portlandoregon.gov/auditservices/article/677598
10 Judith Green and Kevin Pranis, "Gang Wars: The Failure of Enforcement Tactics and the Need for Effective Public Safety Strategies." Justice Policy Institute. 2007.
11 David C. Brotherton, "Education in the Reform of Street Organizations in New York," in Louis Kontos et al eds., Gangs and Society: Alternative Perspectives. New York: Columbia University Press, 2003 David C. Brotherton, Youth Street Gangs. New York: Routledge. 2015.
12 Betsy Gottbaum. "Old Problem, New Eyes: Youth Insights on Gangs in New York City." Offcie of the Public Advocate. 2008. http://www.nyc.gov/html/records/pdf/govpub/moved/pubadvocate/gangs-recs-comboreportfinal.pdf

GANG RAIDS

West Harlem

In 2014, the NYPD, in collaboration with the Manhattan District Attorney's Office, launched a massive gang raid in West Harlem. Hundreds of armed police officers swarmed the Manhattanville and Grant Houses, as well as surrounding buildings, in a coordinated pre-dawn operation. The West Harlem sweep was the largest gang takedown in New York City's history at the time and led to **two indictments of 103 mostly young Black and Latinx individuals.** [13]

Local media outlets appear to have been notified ahead of the raid so as to be prepared for footage of police entering the developments and leaving with handcuffed suspects. The allegation that those arrested were gang members were taken as virtual fact by tabloid and television reporters.

After the raid, several parents of people arrested held a protest outside the Harlem State Office Building. Some said that police pointed guns at them, their children and senior citizens living in the buildings. One mother described her son's arrest:

"They came to my house, raided my house and then they assaulted my son. They kicked him in the scrotum – when he was handcuffed. And he's already sick. Just came out the hospital, they raided my house the next day on June 4th and they kicked him in the scrotum when he was down." [14]

Taylonn "Bam" Murphy Jr. was one of those indicted. Murphy's sister, Tayshana "Chicken" Murphy, was killed in a feud between the development. Manhattan District Attorney Cyrus Vance made the connection between Chicken's death and the raid.[15] In interviews for this report, however, Tayshana's father, Taylonn Murphy Sr., criticized the takedowns:

"So I think the narrative they were trying to spin was that we did these raids because these two individuals got killed. And you know my daughter was one of the individuals that got killed. And I found that to be very troubling because you know you're trying to pin a whole neighborhood against me and my family. Saying that you're the reason for 400 police officers coming in to our neighborhood and kidnapping individuals or arresting individuals or detaining individuals and I had to immediately speak out about that. I had to immediately say 'hey listen, the two individuals that killed my daughter were already arrested.' You can't be vilifying a whole neighborhood saying they had something to do with my daughter's death because that's not true."

Mr. Murphy also suggested that the presence of Columbia University – and its expansion via its multi-million dollar Jerome L. Greene Science Center – contributed to the gang takedowns. Columbia's new campus was located next to Manhattanville as a feud between developments grew.[16] The inference by Mr. Murphy and others who spoke out at rallies was that community issues were swept away in the interest of the University and at the expense of residents.

[13] J. David Goodman. "Dozens of Gang Suspects Held in Raids in Manhattan." New York Times. June 4, 2014. https://www.nytimes.com/2014/06/05/nyregion/dozens-of-suspected-gang-members-arrested-in-raid-of-2-harlem-housing-projects.html
[14] Josmar Trujillo. "Harlem Mom Speaks Out Against NYPD, Daily News After Gang Raids." Youtube. June 14, 2014. https://www.youtube.com/watch?v=uyi3tKJthm8
[15] Christina Santucci. "Vance says gang bust tied to 'Chicken' Murphy slay." QNS. June 14, 2014.
[16] Sarah Hayley Barrett. "After Years of Opposition, Columbia University Comes to Manhattanville." WNYC. October 24, 2016. https://www.wnyc.org/story/columbia-university-begins-move-manhattanville-campus/

Mr. Murphy also pointed out that police, in the years before the raid, actually allowed violence to fester, which was a theme researchers heard in other spaces. During a 2017 forum in West Harlem, one young man from the Grant Houses said that when in custody of police officers, he was purposely dropped off in a rival neighborhood. Earlier this year, Brooklyn cops reportedly blared antagonizing "diss" music from their car to tease gang members in a housing project.[17] Mr. Murphy suggested that police could have prevented his daughter's death, but didn't:

They were looking and watching what these young people were doing. They were allowing them to hurt one another. I know that for a fact because 15 minutes before my daughter was killed, we had a VIPER room officer in the VIPER room looking at these cameras and he watched the young man come out of a totally different building across the street with a firearm, menace a group of other individuals and there was no calling, no intervention.

North Bronx

On April 27th, 2016, the NYPD and several federal law enforcement agencies executed another large gang takedown operation, this time in the Bronx. The raid, the result of **two indictments including 120 defendants** surpassed West Harlem to become the biggest gang raid in New York City history. Emails obtained by a journalist showed Immigration and Customs Enforcement's (ICE) Homeland Security Investigations unit internally discuss the media coverage they expected.[18]

The effect on the ground was, as some residents have described it, like "they were arresting [Osama] bin Laden." Helicopters circled over the Eastchester Gardens housing development. A Homeland Security armored vehicle was driven into the middle of the development's courtyard. A 21-year old man, who mistakenly thought he was a target of the raid, ran from police, climbed out of a window and fell to his death.[19]

The sweep eventually came to be described as the case of the "Bronx 120" by activists and residents, referring to the 120 people accused. A 2019 report from the CUNY School of Law showed that two thirds of those indicted weren't convicted of violence, a third were convicted of Marijuana-related crimes and about half of those indicted weren't even alleged to be gang members by prosecutors themselves.[20]

Instead of local prosecutors, the United States Attorney for the Southern District of New York partnered with the NYPD to bring RICO conspiracy charges. Being charged under the 1970 RICO Act, or the Racketeer Influenced and Corrupt Organizations Act, presented significant challenges for the defendants, including procedural advantages, being retried for past offenses (for which some had already served time) and the prospect of being judged by a federal Southern District jury – which can be a higher-earning, whiter and more police-friendly jury pool than a Bronx jury.

The Bronx 120 takedown become the focus of subsequent stories and films warning of the dangers of police gang labeling and federal RICO laws. Kraig Lewis, the subject of a film, "Trouble Finds You," was arrested in Connecticut the morning of the Bronx raid as he lay in bed with his young son. Lewis was pursuing his MBA degree but instead spent the next 22 months in federal custody after he was initially threatened with capital punishment and then offered lengthy plea deals for crimes he says he didn't commit.

[17] Wes Parnell et al. "Brooklyn Residents Upset at Two NYPD Cops for Antagonizing Gang Members with Controversial Rap Song Blaring from Their Squad Car." Daily News. February 20, 2019. http://www.nydailynews.com/new-york/brooklyn/ny-metro-folk-nypd-rap-gang-20190220-story.html
[18] https://www.documentcloud.org/documents/3475709-ICE-Officials-Discussing-Bronx-Gang-Raid.html#document/p3
[19] Chauncey Alcorn et al. "Robbery suspect falls to his death while running from cops during Bronx gang raids." Daily News. April 27, 2016.
[20] Babe Howell and Priscilla Bustamante. "Report on the Bronx 120 Mass 'Gang Prosecution.'" April 2019. www.bronx120.report.

GANG RAIDS ANALYSIS

Under Mayor Bill de Blasio, the NYPD, along with local and federal prosecutors, launched increasingly larger gang raids based primarily in public housing developments. While difficult to quantify, police officials have testified that in a **two and a half year span over a thousand people were arrested as part of gang investigations.**

Gang raids themselves are violent, dangerous and traumatic experiences for all who experience them. Police utilize assault rifles, battering rams, flash grenades and helicopters. Those affected include neighbors, family members – who have to quickly prepare for debilitating legal battles that can take months, if not years – and the targets themselves. Young children and adolescents, oftentimes the siblings, sons or daughters of those arrested, are almost certainly emotionally damaged by the experience of a police operation. Some can be misidentified as targets, handcuffed and held at gunpoint.

One of the most harrowing and disturbing stories told by West Harlem residents was that of a family whose house was raided and doors knocked off the hinges. One of the children, a sibling of someone arrested, watched as family members argued with officers only to have one officer state that they would be back for him – the younger sibling – in a few years.

The secrecy in the way that gang raids are organized (Who spearheads a takedown – police or prosecutors? What information is shared, including with federal agencies? What personnel, equipment and intelligence are used?), coupled with the state violence that is inflicted, is troubling, to say the least. The tactics are wholly unnecessary and seem to only serve the purpose of a military-like 'shock and awe' campaign against predominantly Black communities.

NYPD GANG DATABASE

The NYPD admits to categorizing local "crews" – smaller, more local and less formal groupings – alongside gangs within its database. Like gangs, "crews" have no consensus definition. Therefore, the NYPD gang database can be more accurately described as a database of people that police believe to be grouped together. **There is no requirement of a criminal conviction, much less a violent conviction, to being added to the database.**

The NYPD began using its database, or what it calls its **Criminal Group Database**, in its current form in 2014. The size of the database is a source of debate – estimates have put the database over 40,000 while police claim it's around 17,000 – and information has been guarded by the police department. Nonetheless, thanks for freedom of information requests, some data exists.

Gang Database Figures

Prior to 2014, CUNY School of Law professor Babe Howell received data from the NYPD indicating that over 20,000 people were added into the NYPD's gang database between August of 2003 and August of 2013, **99% of whom were non-white**. The racial breakdown of NYPD gang database then, about **90% Black and Hispanic**, mirrored the racial breakdown of people who'd been stopped and frisked by police during that same span. Alarmingly, **30% of those in the database were children** when added.

New figures from March of 2018 acquired by Howell indicated that over 1**7,000 people were added to the database from December 2013 through February 2018**, mostly under Mayor Bill de Blasio. The rate at which people into the database under de Blasio was 70% higher than that of the previous administration. Of those added, **over 98% were identified as either Black or Hispanic** – an even more racially disparate scenario than from the previous years.

[21] K. Babe Howell, "Gang Policing: The Post Stop-and-Frisk Justification for Profile-Based Policing." 5 Univ. Denver Crim. Law Rev. 1. 2015.

HOW IS GANG AFFILIATION DETERMINED BY POLICE?

While almost no one outside of the police department knows who, by name, is on the database, we do know some of the criteria that the police say they use for database inclusion:

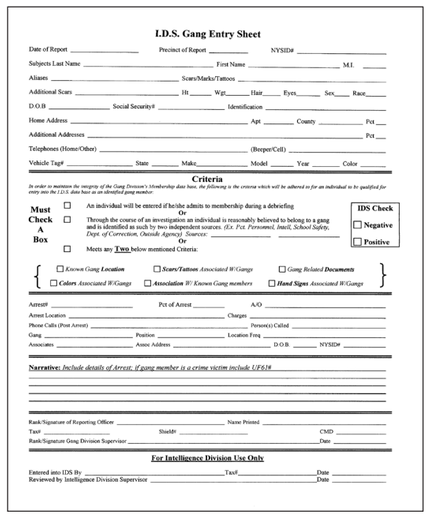
1. **An individual will be entered if he/she admits to membership during debriefing**

   OR

2. **Through the course of an investigation an individual is reasonably believed to belong to a gang and is identified as such by two independent sources. (Ex. Pct. Personnel, Intell, School Safety, Dept. of Correction, Outside Agency) Sources:**

   OR

3. **Meets any two below mentioned criteria:**
   1. Known gang location
   2. Scars/Tattoos Associated with gangs
   3. Gang related documents
   4. Colors Associated with gangs
   5. Association with known gang members
   6. Hand signs associated with gangs



I.D.S. Gang Entry Sheet

Date of Report _____ Precinct of Report _____ NYSID# _____

Subjects Last Name _____ First Name _____ M.I. ____

Aliases _____ Scars/Marks/Tattoos _____

Additional Scars _____ Ht ____ Wgt____ Hair____ Eyes____ Sex___ Race____

D.O.B _____ Social Security# _____ Identification _____

Home Address _____ Apt ____ County _____ Pct __

Additional Addresses _____ Pct __

Telephones (Home/Other) _____ (Beeper/Cell) _____

Vehicle Tag# _____ State ____ Make_____ Model ____ Year ____ Color ____

Criteria

In order to maintain the integrity of the Gang Division's Membership data base, the following is the criteria which will be adhered to for an individual to be qualified for entry into the I.D.S. data base as an identified gang member.

Must Check A Box

☐ An individual will be entered if he/she admits to membership during a debriefing

Or

☐ Through the course of an investigation an individual is reasonably believed to belong to a gang and is identified as such by two independent sources. *(Ex. Pct. Personnel, Intell, School Safety, Dept. of Correction, Outside Agency) Sources:* _____ _____

Or

☐ Meets any **Two** below mentioned Criteria:

IDS Check
☐ Negative
☐ Positive

{ ☐ *Known Gang* ***Location*** ☐ ***Scars/Tattoos*** *Associated W/Gangs* ☐ *Gang Related* ***Documents*** ☐ ***Colors*** *Associated W/Gangs* ☐ ***Association*** *W/ Known Gang members* ☐ ***Hand Signs*** *Associated W/Gangs* }

Arrest# _____ Pct of Arrest _____ A/O _____

Arrest Location _____ Charges _____

Phone Calls (Post Arrest) _____ Person(s) Called _____

Gang _____ Position _____ Location Freq ____

Associates _____ Assoc Address _____ D.O.B. _____ NYSID# _____

Narrative: *Include details of Arrest; if gang member is a crime victim include UF61#*

Rank/Signature of Reporting Officer _____ Name Printed _____

Tax# _____ Shield# _____ CMD _____

Rank/Signature Gang Division Supervisor _____ Date _____

For Intelligence Division Use Only

Entered into IDS By _____ Tax#_____ Date _____

Reviewed by Intelligence Division Supervisor _____ Date _____

Self admission

While admitting to being in a gang to a law enforcement official can be a surefire way of being designated, there are questions with this criteria: is there a process for corroborating what police say was admitted to them? Can or should an individual make an admission without an attorney present? Since "debriefings" – which we understand to be informal interrogations – don't necessarily occur during arrests, are Miranda rights read and are people allowed to contact their attorneys or, if a minor, their parents?

There is also the question of the validity of admissions, particularly for young people. Bragging and overstating one's position in a gang, the legitimacy of a gang (i.e. a group of friends that calls themselves a 'gang') or claiming that one's crew of friends is tough or rich can be based less on reality and more on a fictional projection for those who seek value in street culture. What safeguards are in place to ensure self-admission statements are not coerced or fabricated, like false confessions?

Recently, there appears to have been a dangerous expansion of the self-admission criteria: During testimony to the New York City Council on June 13th 2018, NYPD Chief of Detectives, Dermot Shea, added **"social media post admitting to membership in a gang"** to the criteria.

Police interpretation, or perhaps willful misinterpretation, of gang admission on social media can include emojis, hashtags, or other forms of communication. There is also the question of how police can authenticate who is posting or operating a social media account. Making matters worse, the use of social media posts as a way to authenticate gang membership significantly expands an already questionable process by turning the internet into a virtual police precinct.

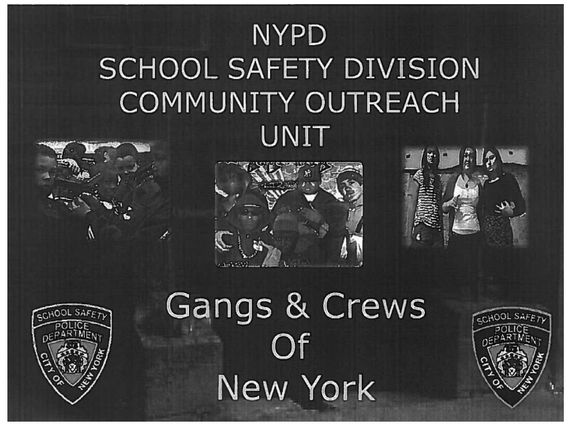
Self-admission can be influenced by the disproportionate power imbalance between an individual, especially a minor, and a police officer. Gang, crew and urban cultures

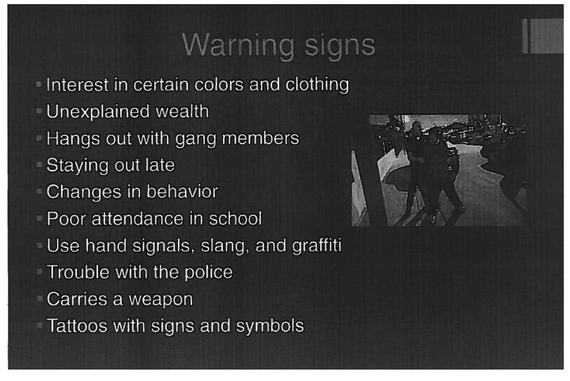
are also susceptible to racial prejudices by police as well as braggadocious exaggerations by those targeted.

Independent sources

"Independent sources," like self-admission, can lead to inclusion on the gang database. However, "independent sources" are not independent. Some listed examples, included **"Pct. Personnel, Intell, School Safety, Dept. of Correction, or Outside Agency."** However, precinct personnel (Pct. Personnel), the NYPD Intelligence Division (Intell) and School Safety Division are all part of the police department.

As part of other Freedom of Information requests made by the Legal Aid Society, materials that appear to be used in training **School Safety** agents to identify gang-involved youth, show troubling parameters: "warning signs" to look out for include "unexplained wealth" (prejudicuous socio economic assumptions), "trouble with police" (ill-defined and potential proxy for race) and "changes in behavior."





The **Department of Corrections** (DOC) has its own internal gang tracking system, the Gang Intelligence Unit (GIU). Because DOC oversees a confined population that often has to associate with gangs and others for safety, gang designations can be more overreaching – and follow individuals after they leave jail.

The final corroborating source is the superfluous **"outside agency."** Do these include state-level or federal law enforcement agencies, some which maintain national databases of their own? Does mutual information sharing between the NYPD and these agencies readily occur? Chief Shea testified in 2017 that the NYPD gang database is not shared outside the NYPD but acknowledged that gang investigations are done in collaboration with federal agencies, casting doubt on those claims.

Another potential source for gang labeling are **Neighborhood Coordination Officers** (NCOs) from the "neighborhood policing" efforts that have expanded in recent years. After a high profile killing of a teenager in the Bronx by alleged gang members, it was local NCOs that led public meetings encouraging community members to watch out for gang activity. According to the NYPD patrol guide, NCO's have access to schools and watch for "problematic conditions, violent crime, and gang/crew activity."

Other criteria (must meet two)

The third pathway into the gang database lays out six options, two which need to be included. **"Known gang location"** and **"associate with known gang members,"** are likely to be affected by housing segregation and offer considerable overlap in public housing developments, where families share common space and build friendships from childhood. A 2015 New York Daily News gang map[22] published using data from NYPD's Juvenile Justice Division provides a glimpse "known gang locations," according to the department:

Credit: New York Daily News

Since most of the areas marked as gang territories by the NYPD are areas with higher concentrations of Black and Latinx populations, a "known gang location" (fulfilling half of the criteria towards gang designation) can serve as a proxy for race. So-called associations might mean shaking hands, talking to or being connected on social media. And, as the city has expanded surveillance of public housing, adding over 4,000 cameras in NYCHA since 2014, public housing is further magnified.[23]

Other options for fulfilling the third criteria include **"scars/tattoos associated with gangs"** and **"colors associated with gangs."** While people can age out of gang involvement, few can remove tattoos, making them problematic signifiers of gang activity. In other states, federal law enforcement use of tattoos in making gang designations have been the subject of lawsuits.[24]

NYPD Testimony at City Council Hearing, June 13th 2018

"Criminal groups that operate on our streets are drivers of a significant portion of violent crime in the city, and some are prime peddlers of narcotics which drive the subsequent increase in opiate overdoses plaguing our city.

While New York City is the safest big city in the nation. In some cases, criminal groups hold pockets of our city hostage, inhibiting mothers from letting their children play outside, or preventing the elderly from taking walks in the neighborhoods."

—Dermot Shea, NYPD Chief of Detectives

At a 2018 City Council hearing, top NYPD officials invoked the language of mass incarceration, even tying gangs to the opiate epidemic, as they provided insight into how police label and catalogue gang members:

Chief Shea explained that one **Field Intelligence Officer** (FIO) is typically assigned to every NYPD command, accounting for about 100 FIO's across the city. FIO's are empowered to make "formal recommendation required in a written narrative in

[22] New York Daily News. "Gangs of New York and How Close You Live to Them." New York Daily News. 2015. http://interactive.nydailynews.com/2015/12/gangs-of-new-york-city-interactive-map/
[23] New York City. "De Blasio Administration Announces Completion of Camera Installation at 22 NYCHA Developments." New York City. June 7, 2017. https://www1.nyc.gov/office-of-the-mayor/news/396-17/de-blasio-administration-completion-camera-installation-22-nycha-developments
[24] Derek Hawkins. "Bad news for the Juggalos: The FBI's gang label could be here to stay." Washington Post. December 19, 2017. https://www.washingtonpost.com/news/morning-mix/wp/2017/12/19/bad-news-for-the-juggalos-the-fbis-gang-label-could-be-here-to-stay/?noredirect=on

supporting documentation that justify each individual's inclusion. **Gang Squad** officers from elite units (i.e. Manhattan North Gang Squad, Queens Gang Squad, etc), who have final say on gang designation, do not report to precincts and operate outside of traditional structures. The **Social Media Analysis and Research Team** similarly works under a shroud of relative secrecy and can make recommendations for inclusion."

During the testimony, Chief Shea also elaborated on other "independent sources" the department may use to designate a gang member, suggesting a long list:

"It could be a confidential informant. It could be the member's parent, which happens. It could be a teacher. It could be people that live on the block and could be a crime victim if we can substantiate it. There's many different examples."

Shea also described "off ramps" for removal: a new review every three years and on an individual's 23rd and 28th birthdays, simply no longer being deemed a gang member, "no police contact or arrest for 3 years" (meaning a single stop or arrest could keep someone in the database) and death. The NYPD claims that thousands have been removed from the database.

GANG DATABASE ANALYSIS

The NYPD has claimed that people on the gang database aren't chosen for frivolous reasons, have extensive criminal histories and many arrests. They don't say whether those arrests resulted in convictions or are indicative of harassment precisely because of their gang designation.

And with the unilateral power to designate people as gang members, the police department also has the power to designate some crimes as gang-related or gang-motivated, allowing them to potentially control gang crime statistics.

On the other hand, the police department has said that the white nationalist group Proud Boys, who describe themselves as a gang, are not in the database and refuse to acknowledge whether traditional Mafia organizations are included. The NYPD doesn't appear to differentiate between a local "crew" of mostly young men of color from the Mafia when they work to bring conspiracy charges devised precisely for those traditional organized crime syndicates.

Investigations into gang databases elsewhere have uncovered wildly inaccurate information, racial bias and abusive and illegal practices:

- **A recent report by the Chicago Office of the Inspector General found that the Chicago Police Department's database was filled with inaccuracies, was shared with immigration officials, and "potentially undermines public confidence in the Department's legitimacy and effectiveness in the service of its public safety mission."[25]**
- **An audit of the Cal Gang database by the California State Auditor found wild inaccuracies in the database including the presence of infant children and raised concerns regarding fundamental privacy protections.[26]**
- **A review of the UK's Gangs Matrix system by Amnesty International found similar privacy issues based on evidence that data was shared with other government agencies affecting people's access to basic government services and employment. Like the NYPD's gang database, the majority of those in the UK's Gangs Matrix were people of color with little or no criminal history.[27]**
- **In Portland, OR, police decided to end the use of their database in 2017 rather than reveal its inner workings when requested to do so by local journalists.[28]**

Gang policing personnel are also a concern. Studies show gang unit cops exhibit "extreme bias," regardless of bias training [Sim, Correll et al, 2013] and a New York Times article says police misconduct data show NYPD gang cops have been "sued for misconduct more frequently than most patrol officers."[29] A recent search of eBay, the online vending platform, shows commemorative pins and coins from NYPD gang units adorned with images of skeletons, grim reapers and machine guns – showcasing a disturbing mentality.

The NYPD, however, says its database is a part of its **"precision policing"** efforts that allow them to narrowly target those most likely to be involved in serious and on-going criminal activity. Instead, the constant surveillance, inclusion in conspiracy cases, enhanced criminal penalties and other consequences that relate to the database outline a strategy of racialized suppression that undermines safety for the communities that police claim they are working to serve.

INVENTING GANGS

While the police department has offered limited testimony on the process of entering an individual into the gang database, little is known about how police validate what is or isn't a gang. It is hard to tell what gangs are real, imagined or manufactured partly because there is no way to challenge a gang's existence – raising the question of whether police could invent a gang.

Oww Oww

The "Oww Oww Gang" was classified as an inactive Brooklyn gang by the NYPD Intelligence Division in 2015. However, residents of Brooklyn's Gowanus Houses, where the gang is said to be based, say that the "gang" doesn't exist.[30] "Oww Oww" was the name of an amateur hip-hop song and video popular in the Gowanus and Wyckoff Houses.[31]

Ronnie Williams was one of the young men from Gowanus that was convicted and alleged to be in the gang. His mother explained how that gang label was fixed onto her son:

"As far as I remember, as soon as it started happening they tried to paint him as a gang member. They started saying outwardly [inaudible] referring to him as a "gang member". When he would hang out with his close friends at the time Dante and one of his other really close friends named Nunu, and he was a rapper... So he [Nunu] wrote

---

[25] Office of the Inspector General. "Review of the Chicago Police Department's 'Gang Database," City of Chicago Office of Inspector General. April 2019.https://www.documentcloud.org/documents/5816977-OIG-CPD-Gang-Database-Review.html.
[26] California State Auditor. "The CalGang Criminal Intelligence System," California State Auditor. August 2016. http://www.voiceofsandiego.org/wp-content/uploads/2016/08/CalGangs-audit.pdf
[27] Amnesty International. "Met Police Using 'Racially Discriminatory' Gangs Matrix Database," Amnesty International. May 9, 2018. https://www.amnesty.org.uk/press-releases/met-police-using-racially-discriminatory-gangs-matrix-database
[28] Carimah Townes. "Portland is Saying Goodbye to its Controversial Gang Database." The Appeal September 12, 2017. https://theappeal.org/portland-is-saying-goodbye-to-its-controversial-gang-database-e88e6c05262c/
[29] Ali Winston. "Looking for Details on Rogue N.Y. Police Officers? This Database Might Help." New York Times. March 6, 2019. https://www.nytimes.com/2019/03/06/nyregion/nypd-capstat-legal-aid-society.html
[30] Josmar Trujillo. "Brooklyn's Wrongful Convictions Persist With 'Gang' Cases." Huffington Post. February 17, 2018. https://www.huffpost.com/entry/brooklyns-wrongful-convictions-persist-with-gang_b_59610852e4b085e766b5131d?guccounter=1
[31] Ill Flo. "nu money - nu nu - oww oww official video" YouTube. July 5, 2011. https://www.youtube.com/watch?v=1rHUgIF1T3M

the song about Gowanus and called it Oww Oww. So they [police] used that to say, like, that was an anthem for their gang."

Williams' sister disputed her brother being in a gang as well as "Oww Oww" being an actual gang:

"That song became really popular in the community and people would walk by each other and say Oww Oww just because it was Gowanus' song. But they took that and said that all of those guys who would rep the song, that was a gang. And the name of the gang was Oww Oww... But that would only come from people who weren't from Gowanus."

Music, Hip-Hop in particular, has been used by law enforcement as evidence and markers of gang violence. Rap lyrics have even been used as evidence. However, in the street and Hip-Hop culture, attaching the word 'gang' to a group of people or even a song is common but doesn't signify an organized criminal enterprise. The prevalence of young people posting about or framing community relationships as a "gang" isn't new, can easily been misconstrued, and shouldn't be the impetus for the classification of a gang or crew by law enforcement. [32]

Chico Gang

In February of 2019, a dozen young men in East Harlem were arrested and charged with gang conspiracy, among other allegations, and accused of being members of the "Chico Gang." According to the NYPD and Manhattan District Attorney Cyrus Vance, the "gang" was based in the Wagner Houses and formed after the shooting death of Juwan "Chico" Tavarez in 2016.[33]

However, several residents of the Wagner Houses said they weren't aware of such a gang. Some were familiar with the sayings "Chico Gang" or "Chico World" that became popular in Wagner amongst friends and classmates of Tavarez. There is also no public record of the gang in media articles before the arrest or even in the most recently available NYPD gang map.

While residents reported that classmates wore lanyards with large pictures of Juwan after his death, this could have been an indicator, to police, of involvement in the dubious "Chico Gang." In one Manhattan courtroom, NYPD detectives on a different case testified that they looked at people wearing similar commemorative pictures "more closely" when looking for retaliatory gang violence.

In a statement from Vance's Office, authorities referred to the defendants discussing criminal activity on social media as part of the case against them.[34] However, the mining of social media posts, an arena where adolescents and young adults may not understand the implications of what they post and where law enforcement is free to infer whatever meaning helps a criminal case, is a recipe for abuse.

A social media search on any given day can find hundreds, if not thousands of posts referencing a gang, most of which are clearly not related to organized crime. In New York City, police even use emojis to decipher gang identities and threats of gang violence.[35]

[32] Stephanie Clifford. "Artist or Gang Leader? Rapper's Trial Begins." New York Times. May 27, 2014. https://www.nytimes.com/2014/05/28/nyregion/rappers-federal-racketeering-trial-begins.html
[33] Noah Remnick. "A 16-Year-Old Boy Killed, and an East Harlem Neighborhood's Grief." New York Times. March 28, 2016. https://www.nytimes.com/2016/03/29/nyregion/juwan-tavarez-16-killed-an-east-harlem-neighborhoods-grief.html
[34] Manhattan District Attorney. "DA Vance and Police Commissioner O'Neill Announce Indictment of 12 Members of East Harlem 'Chico Gang'." Manhattan DA's Office. February 8, 2019. https://www.manhattanda.org/da-vance-and-police-commissioner-oneill-announce-indictment-of-12-members-of-east-harlem-chico-gang/

In fact, while there is a growing amount of research dedicated to deciphering how social media relates to gang violence, little, if any, has sought to separate public expressions of 'gangs' to actual violence.

Amongst youth, words are fluid and meant to be accessible to many. Police can, however, wittingly or unwittingly take dangerous liberties by ascribing criminality or violence to these expressions. One recent report found that police "massively overestimated the direct linkage between what someone does online and what someone does offline."[36]

Did the Chico Gang ever exist? What is clear in interviews with residents of Wagner Houses is that the community was hurt by the loss of Juwan Tavarez. Notably, some of the charges against those alleged to be in the Chico Gang went back as far as 2015 – before Chico was killed and the gang could have existed.

CONSEQUENCES OF BEING GANG LABELED

Harassment & hyper-policing

One of the primary consequences of being labeled a member of a gang by the NYPD, whether formally in the gang database or even informally amongst gang unit and precinct officers, is heightened **harassment and hyper-policing**. Police interactions, despite an overall decrease in reported stops in New York City in recent years, continue to have a disproportionate impact on communities of color – and this could be more pronounced for alleged gang members.

Street-level contact with police has been a constant theme amongst community residents who were interviewed for this report, specifically mothers and grandmothers. In one interview, a 61-year old woman from East Harlem's Jefferson Houses described prior harassment of her grandson by police officers from the local housing police unit, PSA 5:

"They start gathering the information of how old you are around 14 or 15. They start stopping you–now they can't stop you anymore –I don't know what they gon' do. But they stop you. "How old are you?" take you to the precinct—your mother gotta come and get you –you know, stuff like that."

With more policing and more arrests came deeper forms of harassment. Police officers would search for her grandson in her apartment, she said. He was arrested several times, including once, she alleged, over a robbery simply because he and his friends were in the vicinity of the incident. That arrest would derail his education, preventing him from graduating high school because he was sent to Rikers Island just before his final Regents high school exam, she said. Ironically, in Rikers, he was continuously assaulted because he didn't belong to a gang.

"So...they unfairly label us –them–as gang members. You know I told them he's not a gang member. He hangs out with friends he grew up with. How's that a gang? You have 5 people sitting right here—what are you? A gang? They know each other. They known each other all their lives."

---

[35] Sara Dorn. "New York gangs are using emojis as a secret language to plan crimes." New York Post. August 3, 2019. https://nypost.com/2019/08/03/new-york-gangs-are-using-emojis-as-a-secret-language-to-plan-crimes/
[36] Chip Mitchell. "Study: Cops Overstate Effects Of Social Media On Chicago Gang Violence." WBEZ. May 10, 2019. https://www.wbez.org/shows/wbez-news/study-cops-overstate-effects-of-social-media-on-chicago-gang-violence/7f3e77f9-ba83-429b-98b2-2df1bd4ade49

In a 2015 New York Times article, the focus by police on individuals who they deemed gang-involved was described through the story of a young man from the Brownsville section of Brooklyn named Alexander Williams.[37] Mr. Williams had been arrested numerous times and was one of a few hundred individuals that police were now targeting to combat violence, some of whom were now targets of the policing of smaller offenses, like jaywalking.

"Their names and faces are distributed to precincts across the city. Their gang affiliations and Instagram postings are studied by officers. They are repeatedly arrested, stopped or given tickets, including violations for minor offenses like jaywalking.

Mr. Williams, in an interview, described a smothering police presence in his life that 'does not stop.' Twice, he said, he has been cited for jaywalking. He denied that he was a member of a gang or that he committed the crimes the police have alleged."

Williams and his friends were often arrested but the charges were almost just as often dismissed. This approach is consistent with the NYPD testimony at the City Council that those on the gang database had on average of over 11 arrests, five of which are felonies.

For another Brooklyn resident, hyper-policing preceded a serious gang charge. Ronnie Williams was alleged to be a member of the "Oww oww" gang (see Sidebar: Inventing Gangs). He was convicted and sentenced for what prosecutors said was his role in a shooting. In interviews for this report, however, Williams' mother, Diana, and sister, Shaniqua, say that he was not a gang member and was unfairly swept into an indictment by officers from the 76th precinct who had targeted him for years. His sister explained how her brother felt the need to run from police from an early age:

"He told me on one Halloween he was probably 14 or 15 he and his friends were out trick or treating and they started throwing eggs at each other [inaudible] and he said that the cops came and he did like the whoop sound as a warning signal to let people know that they were there and they just kept playing and whatnot and eventually they started to walk away because the cops didn't leave and he said that he looked back and that they were still following him and he just started to run and he said he ran for a long time. They just kept chasing him. Finally he had to stop because he has asthma. He couldn't breathe. So he just sat in between 2 cars on the curb and he said that the cops came up to him with their guns out telling him to put his hands up for no reason."

That arrest, she says, marked a pattern of unwarranted attention from cops that began to become more personalized. After chasing him on another occasion, cops said "Oh, you're pretty fast, huh?" While it is not clear if the NYPD tagged Williams a gang member at a young age, their gang database has included hundreds of entries of minors.

As Williams got older, his mother said, his interactions with police become more serious, including once when officers assaulted him in the hallway of their building. She described probing visits from police when Williams was 16 or 17 years old. In one example, she described a visit from police who wanted to see her son because, they said, people claimed that he had guns in the house.

On the day he was arrested for the charges he'd face in 2016, she said, police knocked on her door and she asked to see a warrant, wary of riot gear-clad cops standing in her hallway. One officer insisted on showing her the warrant – inside. When she opened the door to let one officer in to show her the warrant, all the cops stormed in, ransacked the apartment and arrested her son. She never saw the warrant.

Gang labeling by agencies outside of the police department can also escalate relatively routine encounters with police, such as a car stop. Victor Dempsey, community organizer with the Legal Aid Society, left the Bloods gang in 2014 when he was 19 years old after serving time for attempted robbery. In 2017, however, after being pulled over failure to signal, a minor infraction, NYPD officers handcuffed him and put in in their squad car.[38]

From the backseat of the police car, Dempsey says he saw "security risk group" on the police computer next to his old mugshot. Security Risk Groups are gangs tracked throughout the jail system by the Department of Corrections Gang Intelligence Unit (GIU).[39] The NYPD's access to Dempsey's DOC gang designation (which suggests his gang status hadn't changed in 13 years), dramatically altered the encounter.

Enhanced bail

The problems presented by hyper-policing are compounded when community members labeled as "gang" affiliated reach the court system. In New York, accused persons must be brought before a judge for a bail hearing within 24 hours of their arrest. Judges are only permitted to set bail to ensure that a person returns to court. Historically in New York courts have been permitted to consider an accused person's "character, reputation, habits and mental condition" when determining how much bail to set.

This provision of the bail law allows prosecutors to take the NYPD's gang designation and bring it into the courtroom.

When a prosecutor alleges that someone has gang affiliations, it often results in judges setting high bail, far higher than would be necessary to merely ensure a community member's return to court. Judges frequently assume "gang member" to mean a person is dangerous or regularly engages in criminal activity. It could also suggest willingness to intimidate, tamper with, or harm witnesses, particularly where someone has been harmed as a result of the alleged crime. While judges are not supposed to factor in these considerations under the law, in reality they are very concerned about releasing someone they perceive to be dangerous. As one defense lawyer who took part in a survey for the report explained, just alleging gang affiliation can change the bail decision for people they represent:

"The simple allegation that a person is affiliated with a gang, even when it is merely asserted by a prosecutor and even when it is disputed by a defense lawyer, greatly increases the chance that bail will be set and the amount of bail."

Another attorney put it more succinctly, "Judges freak out when they hear it." While another stated, "it's extremely harmful and difficult to refute." One attorney reported asking a judge to lower the bail amount for a seventeen year old because her client's family could not afford the amount. After calling the prosecutor and defense lawyer to the bench, the judge commented off

[37] J. David Goodman. "As Shootings Rise in New York, Police Focus on a Small Number of Young Men." New York Times. July 21, 2015. https://www.nytimes.com/2015/07/22/nyregion/as-shootings-rise-in-new-york-police-focus-on-a-small-number-of-young-men.html

[38] The Takeaway. ""All this time went by and I'm still in a database": Questions Arise Regarding Police Gang Databases." WNYC. July 10, 2018.

[39] Shelly Feuer Domash. "Working Gangs From Inside Prison." Police: The Law Enforcement Magazine. May 1, 1999. https://www.policemag.com/338700/working-gangs-from-inside-prison

the record in a concerned tone that the previous judge had written "Trinitario" on the court file. The judge denied the request to lower bail.

The NYPD "gang" designation follows people into the criminal legal system, disadvantaging them from the initial bail decision onward. By using a gang affiliation to request high bail, prosecutors ensure that a person is deprived of their liberty pre-trial. Judges and prosecutors know that people subject to the violence of incarceration are more desperate to secure their release through cooperation with an investigation. For example, Afrika, a young woman from Harlem, had bail set in a gang conspiracy case. When supporters from her church community attempted to pay the bail, the judge would not approve the bond.

"Their idea was that I was gonna get locked up, I was gonna be facing this bail issue and then because I was gonna be under pressure I would cooperate and the case would be done."

Beginning January 1, 2020 consideration of an accused person's "character, reputation, habits and mental condition" has been removed from the bail law. Though the new law does not prohibit prosecutors from raising this via an alleged gang affiliation or judges from considering it, defense lawyers have strong arguments that the legislature removed this language precisely because of the discriminatory manner in which it was being used. In reality it is likely that prosecutors will continue to use an NYPD gang designation in bail arguments and judges will continue to be biased by it. With high or no bail, defendants are further pressured to take plea deals, become cooperating witnesses, or both.

Indictments, Trials, and Plea Deals

In a survey for this report, defense attorneys and public defenders reported the influence of gang allegations in courtrooms:

"In many cases, an allegation of gang membership is not an element of a charged crime. In bail applications, prosecutors will simply assert that they have information that a person is a gang member without revealing their sources. We are left to fight blindfolded against the gang allegations. Police can also get young people to admit to "gang affiliation" if they know anyone who is in a gang even when they aren't in gangs themselves.

Because many teenagers in the Bronx know SOMEONE in a gang or have some family member in a gang, it's very easy for police and prosecutors to claim that they are "gang affiliated." Teens are then treated as guilty by association without the prosecution needing to prove that they have done anything wrong. Young people in poor black and brown communities specifically end up being targeted and harmed by this practice."

Few terms can color a courtroom like the word 'gang.' As another defense lawyer put it, "being in a picture with friends from your neighborhood sometimes seems like sufficient [probable cause] for an indictment." The power of a gang allegation also affects plea offers from prosecutors, according to another defense attorney:

"In the Bronx, cases that involve allegations of gang affiliation often go to the same courtroom/same judge -- this courtroom and judge are notoriously pro-prosecution, speedy trial and discovery rights are completely ignored, and clients get bullied into cooperating or taking unfavorable pleas."

Trials present more problems. Indictments are obtained by offering cooperation agreements to individuals who have already been charged with serious violent offenses if they tie other alleged members of the group to various crimes. Defendants are then often brought up on "conspiracy" charges as a way to admit evidence that is excessive, irrelevant, and not from a credible source, in order to inflate sentencing and charges.

As one juror on a gang trial put it, "conspiracy charges were wide enough to drive a bus through," referring to the expansive definition of what constitutes "conspiracy. In this context, juries may wind up finding someone guilty without agreeing on what exact crime they are guilty of committing.

In the trial of a 36-year old father from the Bronx, whose family says had long been harassed by cops from the 47th precinct, federal racketeering charges were brought largely because of his relationship with a co-defendant, who was also a childhood friend. Hearsay testimony and old arrests, including some that were dismissed, were presented as evidence. The jury, on the other hand, wasn't allowed to hear the full misconduct history of one of the detectives whose testimony proved vital to the prosecution. This detective who made the arrest had at least eight federal civil rights lawsuits filed against him, four totaling about $235,000 and three for undisclosed sums. The jury was only told about one.

This man's mother believes the local precinct put her son on the gang indictment because of his past complaints and lawsuits against some of these officers. She was also frustrated by testimony from government witnesses:

"So they all get to use that RICO conspiracy to to tie them into making this a bigger case. But what I'm seeing is that what they want people to do is they use other people who are un-credible... on another case that could be, uh, incarcerated somewhere. So they're going to use them and they bring them like 'Hey, do you know these young men? Gimme something on them, work with us.' They could say whatever they want to say. I mean, they're in a situation to say, 'You know what, I'm going to get a sweet deal to get home.'"

To juries, accusations of gang membership can be confused with the crime of conspiracy – a major problem that threatens freedom of association. Since conspiracy charges need to prove the element of agreement to commit a crime, prosecutors may try to prove this agreement by emphasizing that by associating, defendants are tacitly "agreeing" to criminal acts. However, association is not a crime, and does not prove an agreement or intention or even gang membership: gang members and non gang members are part of the same communities, neighborhoods, and families.

In practice, prosecutors often succeed in proving that defendants are part of a conspiracy by introducing evidence that should merely prove that they know each other; the jury is shown countless social media posts and messages. Prosecutors intentionally blur the line between conspiracy and association. After presenting posts and private messages, their content is often "translated" either by gang experts (police officers involved in gang policing, not necessarily with any education or background) or by police cooperators and informants.

Posts can contain rap lyrics and quotes, which are then presented to the jury as matter-of-fact statements made by the co-defendants. Additionally, gang experts may say that they understand the slang used by defendants, but there's no protocol in place to ensure that evidence is interpreted correctly. In one interview for this report, a

mom described how a picture her son posted of himself holding money was presented in court to suggest he was a drug dealer:

"They took that and said, oh, he's a big-time drug dealer. They criminalize him in any photograph that he had. Not knowing the story where that came from that known what that meant to him and to be able to hold his son to say, I have a son, you know, I'm able to support my family, you know, um, how they pose in pictures and whatever to the message is misconstrued in that sense."

Jury members have to endure weeks or months of this. What results is a general atmosphere of criminality, built by prosecutors, that serves to convince juries less of what crime the defendants are accused of and more that they are associated with a criminal world and therefore must be guilty of something.

Individualized justice is not afforded to people who are connected to gangs and to the alleged behaviors of their co-defendants – who are oftentimes friends and peers but in some cases can even be virtual strangers. In this context, along with the pressures of being incarcerated often without bail, many feel compelled to plead out, boosting conviction rates and creating the impression that collective punishment is in fact producing justice.

Employment Issues

The NYPD claims that it does not share any information about who is in the database with other agencies, employers, or members of the public. However, in one case reported by the Legal Aid Society, a young person who had been hired for a city position and was undergoing training, was fired because they were in the database. In an interview with a young woman indicted in a gang conspiracy case in Harlem, she reported that she was turned down for jobs because of her gang designation even after he returned from prison.

In these cases, it appears that the gang database may have been used as part of a background clearance. This raises substantial questions about how the database is being used within city government. Is this standard practice for city employment? What safeguards are in place to prevent the NYPD from formally or informally sharing information for the database? There is a long history of police agencies unlawfully sharing information from various types of intelligence files with employers, like the so called "red squads" for much of the 20th Century.[40]

Housing

Gang takedowns in New York City appear to predominantly target public housing and surrounding communities. In addition to the impact of the criminal justice system, public housing residents and their families face an additional challenge: permanent exclusion.

Spurred by the federal Housing Opportunity Extension ("H.O.P.E.") Act of 1996 – or what is more commonly known as the "One Strike, You're Out" policy – the New York City Housing Authority (NYCHA) has developed policies to evict public housing residents based on contact with the criminal justice system. During his 1996 State of the Union address, then President Bill Clinton encouraged states to get tough on gangs and drugs through the zero-tolerance approach embodied by HOPE.

Promoted as a policy to improve "safety and security of its residents," NYCHA uses permanent exclusion is one aspect of these efforts at the local level as it seeks to bar people arrested for certain offenses from residing or even visiting NYCHA property.[41] Exclusion efforts begin when the agency files a "termination of tenancy" action when a tenant or "someone under the tenant's control" takes part in "dangerous conduct."

As local reporting has shown, tenants, sometimes a parent or guardian of a targeted individual, are compelled to exclude family members in order to avoid eviction. As part of the agreement with NYCHA to stave off eviction, (a process in which some residents don't know they're entitled to a lawyer), the apartment is subject to random inspections by the agency. If an excluded person is found in the apartment, eviction proceedings can begin.[42] From a 2015 City Limits article:

Some of the main criticisms of NYCHA's exclusion policies, and the federal strategy more broadly, is that exclusion efforts and perceived levels of "dangerousness" are shaped by arrests, not necessarily convictions, and that less evidence is needed to exclude or evict because proceedings are civil, not criminal.

NYCHA officials, however, have touted the tactic as an "alternative" to eviction, which could put an entire family at risk. During 2017 testimony at a New York City Council hearing, NYCHA officials remarked about "saving" the tenancy of an elderly grandmother whose grandson had been indicted as part of a 2015 federal gang takedown. They apparently saved her by barring her grandson and leaving her at risk of eviction should he ever visit. It also elevated his risk of homelessness.

Eighteen months after the 2014 West Harlem gang raid, NYCHA had already attempted to kick out at least 28 defendants from the case, successfully excluding 17 of them.[43] While the total number of exclusion proceedings as a result of gang enforcement is not known, gang takedowns can often lead to exclusions because of the seriousness of the charges that accompany them and because most takedowns seem to be centered in public housing. Exclusion followed the mass 2016 gang raid in the Bronx. From *The Intercept*:

"After the Eastchester Gardens raid, many families whose sons had been arrested received letters notifying them that NYCHA had initiated termination proceedings against them. Mattison said she had been late on rent, but that housing officials told her she had broken the lease by letting one of her sons and her granddaughter's father stay at her apartment without declaring it. Because they were now caught up in a federal case, she said they told her, the whole family had to go.

A spokesperson for NYCHA told The Intercept that when the agency learns of the arrest of an individual with connections to public housing, it opens a "rigorous and comprehensive investigation." In the Eastchester Gardens case, officials identified 16 individuals named in the indictment with connections to tenants, leading to two permanent exclusions — an option given to family members to save the tenancy."[44]

Permanent Exclusion came under heightened scrutiny by community organizations and advocacy groups during a 2017 City Council Hearing. Dozens of legal

[40] Alex S. Vitale. The End of Policing. Verso, 2017. In "Ch. 10: Political Policing."

[41] New York City Housing Authority. "Permanent Exclusion – Frequently Asked Questions." https://www1.nyc.gov/site/nycha/residents/permanent-exclusion-faq.page

[42] Batya Ungar-Sargon. "NYCHA Questioned on Policy of Banning Arrested Residents." City Limits. June 2, 2015. https://citylimits.org/2015/06/02/nycha-questioned-on-policy-of-banning-arrested-residents/

[43] Greg B. Smith. "NYCHA's move to permanently exclude criminal tenants appreciated by residents, but difficult process." New York Daily News. November 8, 2015. http://www.nydailynews.com/new-york/nycha-moves-permanently-exclude-criminal-tenants-article-1.2427048

[44] Alice Speri. "In New York Gang Sweeps, Prosecutors Use Conspiracy Laws to Score Easy Convictions." The Intercept. July 12, 2016. https://theintercept.com/2016/07/12/in-new-york-gang-sweeps-prosecutors-use-conspiracy-laws-to-score-easy-convictions/

and community groups criticized the city for pushing residents out of public housing amid a housing crisis. The hearing came as a result of a March 2017 report from the Department of Investigations which chastised NYCHA for not being aggressive enough in its exclusion efforts. The report was fiercely opposed by advocates as "misguided and irresponsible."

The Department of Investigations (DOI), a New York City law enforcement "watchdog" agency, recommended in the report that NYCHA should more aggressively prosecute cases, transfer exclusion powers from NYCHA civilians to law enforcement; and that the NYPD should amend its patrol guide to automatically report off-site arrests (not convictions) and to use its "computerized systems" (perhaps the gang database) to "flag" referrals for exclusion efforts.

DOI, worked closely with the NYPD during a gang raid in Brooklyn's Sheepshead-Nostrand Houses in January 2018. After the arrests, former DOI head Mark Peters encouraged NYCHA to increase not only exclusion but also eviction efforts against family members who "should have known" about alleged criminal activity. Alarmingly, DOI also oversees the Office of the NYPD Inspector General, a police oversight agency which contributors to this report have repeatedly called upon to investigate NYPD gang tactics.[46]

The collaboration between DOI and NYPD on gang sweep exclusions raises questions (If DOI, for example, has used the gang database to expedite NYCHA exclusions) of whether independence exists between DOI and the police department.

Exclusion and eviction pressures triggered by dragnet-like gang prosections target mostly Black and non-white NYCHA tenants, as grassroot groups from the "Stop The Raids" coalition have pointed out.[47] For people who are in the depths of poverty or coming home from prison to piece together their lives, public housing represents one of the only affordable options left in an increasingly unaffordable city.

Deportation risks

In 2017, New York City became a so-called "sanctuary city," which is a municipality that limits cooperation with federal immigration enforcement agencies as a matter of policy. However, the NYPD's collaboration on gang takedowns with the Homeland Security Investigations (HSI) unit, a division with Immigration and Customs Enforcement (ICE), the country's most prominent immigration enforcement agency, may offer a loophole around any sanctuary protections.

While it is not known how many gang takedowns in New York City have led to deportations, the gang label presents serious and unique legal problems for noncitizens. Immigration practitioners report that allegations of gang affiliation based on gang allegations and gang databases are arising in the immigration context when noncitizens apply for immigration benefits, adjustment of status, and as a pretext to initiate removal proceedings.

Almost all defenses to deportation are discretionary, that is, whether in the judge's opinion relief is merited. Most individuals bear the burden of proof to show eligibility, which is an uphill battle. People are being denied based on gang-related allegations. There is no right to counsel, so these allegations are very difficult to challenge.

Further, anyone who is subject to deportation can be detained. Bond hearings are subject to discretionary detention and the burden of proof is on the immigrant to show the merits of a grant of bond. In this context, it is extremely difficult to show that someone is not a danger, especially when gang allegations are brought that immediately prejudice the judge and suggest one has engaged in dangerous conduct. Rules of evidence do not apply, so it is difficult to challenge the various HSI, arrest, and other reports.

After a string of murders in Long Island in 2017, then United States Attorney General Jeff Sessions came to New York to tie the panic around MS-13 to President Donald Trump's immigration enforcement efforts. Clearly, for those dedicated to an even more zealous, cruel and xenophobic immigration policy, the policing and labeling of undocumented and noncitizen community members as gang members serves as an indispensable tool.

SCHOOL POLICING

One of the avenues for ending up on the gang database is through classification by a School Resource Officer (SRO). SROs work for the NYPD and there are over 5,000 of them in City schools, funded out of the Department of Education budget at a cost of $750 million annually.[48] SROs are part of the school to prison pipeline and much of the justification for them has been the fear of "gang violence" in schools.

This had led many schools to become fortified camps with the use of metal detectors, heavy presence of officers and the adoption of a variety of "zero tolerance" disciplinary policies that often result in arrest. These arrests target young people of color almost exclusively, mirroring the racial disparities in the gang database.[49]

These SROs receive specific training on how to identify gang members and associates that rely on superficial assessments. The NYPD and Department of Education recently revised the memorandum of understanding between them regarding the functioning of SROs in schools.[50] While that MOU restricted police powers in important ways, it did not reduce their role in placing young people on the gang database. Additionally, teachers can also be empowered to help make gang allegations.

Further, reports by SRO's are found in immigrant children's immigration files and used as a basis for detaining and deporting immigrant students, particularly Latinx students. Moreover, school district codes of conduct use terms behavior, items, paraphernalia, colors and jewelry as indicators of being "gang related." However, courts across the country, and the United States Supreme Court have repeatedly determined that labeling conduct as "gang-related" is unconstitutionally vague, violating people's rights to notice of how their behavior and or appearance is being categorized. This vague labelling of "gang" without description in school district codes of conduct allows for wide-latitude of discriminatory enforcement against students, especially students of color.

Defining the disciplinary issues in schools as "gang" issues further justifies harsh practices that drive students out of school and into the criminal justice system. In some cases the mere suggestion of gang involvement as indicated by wearing certain clothing, walking to school with a regular group of friends, or sharing an interest in certain music can bring on intensive surveillance in the school and even inclusion on the gang database – which invites intensive police scrutiny outside of school as well.

[45] Emma Whitford. "NYC Agency uses Brooklyn Gang Raid to Encourage Evictions of Entire Families from Public Housing." The Appeal. January, 31, 2018. https://theappeal.org/nyc-agency-uses-brooklyn-gang-raid-to-encourage-evictions-of-entire-families-from-public-housing-46ec51c9362/

[47] Ashoka Jegroo. "With Nighttime Raids, Police Wage War on Black and Brown Families in New York." Truthout. March 31, 2017. https://truthout.org/articles/with-nighttime-raids-police-wage-war-on-black-and-brown-families-in-new-york/

[48] The Center for Popular Democracy and the Urban Youth Collaborative. "The $746 Million a Year School-to-Prison Pipeline: The Ineffective, Discriminatory, and Costly Process of Criminalizing New York City Students." April 2017. https://populardemocracy.org/sites/default/files/Executive%20Summary.pdf

[49] NYCLU. "Criminalizing the Classroom." NYCLU 2007. https://www.nyclu.org/en/publications/report-criminalizing-classroom-2007

[50] Alex Zimmerman. "NYC Announces its First Overhaul of How Police Operate Inside Schools Since Mayor Giuliani." Chalkbeat. June 20, 2019. https://chalkbeat.org/posts/ny/2019/06/20/nyc-announces-its-first-overhaul-of-how-police-operate-inside-schools-since-mayor-giuliani/

FOCUSED DETERRENCE

Since the introduction of the Juvenile Robbery Intervention Program (J-RIP) in 2007, the NYPD has undertaken a variety of "focused deterrence" programs they claim reduce violent crime through the intensive targeting of young people believed to be most at risk of participation in violence. "Focused Deterrence" programs, developed by criminologist David Kennedy and first implemented in Boston in 1996, attempt to stop gun violence or other serious crime through intensive and targeted enforcement combined with support services.

Ideally, this model begins with a community mobilization effort in partnership with local police. The goal is to send a unified message to young people that serious crime will no longer be tolerated. If it occurs, they will use every resource at their disposal ("pulling levers") to not only apprehend the assailant but to disrupt the street life of young people involved in crime across the board.

The theory is that young people will choose to avoid violence so that they can concentrate on socializing and low-level criminality free of constant police harassment. This is based on research that showed that a great deal of shooting was not drug or robbery related but involved a constant tit for tat of revenge gunfire by rival factions of young people engaged primarily in turf battles. The key is to break that cycle of retribution and gun carrying.

To achieve this, young people believed to be involved in violence are called into meetings with local police and community leaders and threatened with intensive surveillance and enforcement if the gun violence doesn't stop. These "call ins" are made possible in part because many of these young people are on probation or parole for past offenses.

In addition to more intensive enforcement efforts, there is usually an effort to develop some targeted social services with the hope that this will help draw some of these young people away from violence and towards education and employment opportunities.

The original J-RIP program, which began in Brownsville in 2007 and expanded to East Harlem in 2009, targeted juvenile robbery offenders who were back in the community.[51] These youths were given a clear message that they were under enhanced police supervision and would face significant consequences if rearrested. They were also offered mentoring and a few support services by police in hopes of steering them in the right direction.

In practice, J-RIP offered little in the way of services. Young people were given a chance to participate in existing programs like the Police Athletic League (PAL) and were regularly visited by uniformed officers in their homes and on the streets. While these officers were supposed to be acting as mentors and monitors, defense lawyers reported that officers sometimes used these visits as a pretext to conduct searches and that they sometimes called attention to program relationships in front of other youth, potentially marking them as informants—a dangerous label in these neighborhoods.

No real services, such as job placement or family counseling were provided, and the officers involved had no special social services training, playing a primarily surveillance and enforcement role.

A November 2014 NYPD evaluation report showed that a decline in robberies in the target area touted by police mirrored city-wide trends and that J-RIP participants were rearrested at the same or higher rates than youth with similar records in the same and nearby neighborhoods without J-RIP.[52] Even though the 2014 report showed there were no crime reductions under J-RIP, the NYPD has moved forward with an expansion of the program in a different guise: Ceasefire.

In early 2015, the NYPD rolled out NYC Ceasefire under the leadership of Susan Herman, Deputy Commissioner for Collaborative Policing. Ceasefire focuses more on gun crimes and adds group "call-in" meetings in which the targeted youth are brought in and lectured to by police and community members about the harmful effects of their violent actions and the potential enhanced consequences of additional violent offenses.

Participants, mostly forced into Ceasefire through parole or probation, are then placed under extensive surveillance regimes and targeted for enhanced punishments if caught re-offending. They are also offered some minimal services, primarily in the form of a centralized referral phone number run by a local non-profit that is there to link young people to already existing programs.

NYC Ceasefire relies on a logic of collective punishment and has been repeatedly cited in press reports as a key anti-gang initiative by the NYPD.[53] While some stories paint a picture of police and sometimes local clergy members performing door to door outreach, defense attorneys have also reported that their clients are receiving letters from the NYPD, alleging they are gang members and threatening them with enhanced surveillance and prosecutions.

After a Ceasefire "call in," any serious crime in the targeted catchment area will trigger a set of enhanced penalties for any young person arrested in that area, even if they were not part of the call in, or otherwise notified. Defense attorneys have reported showing up to court with clients who are facing remand (no bail) and enhanced charges because of the collective punishment approach, even though they have no knowledge of the initiative.

Evaluation research of these programs does show some meaningful declines in crime that can even last for years. Overall, though, the results are quite thin. Most reductions are small, occur in only a few crime categories, and don't last very long. They also continue to reinforce a punitive mindset about how to deal with young people in high crime, high poverty communities, most of whom are not white.

There are also other emerging "deterrence" programs focused on small groups that are outwardly punitive and arguably allow police to overreach their authority. Project Fast Track, announced in 2016, was launched as a collaboration between police, prosecutors and federal law enforcement agencies to "speed up" gun possession cases in New York.[54] The explicit goal was to produce more convictions – and faster. The NYPD unit created to produce better cases, the Gun Violence Suppression Division, has been profiled as a leader in anti-gang policing.[55]

FOCUSED DETERRENCE ANALYSIS

"Focused deterrence," relies primarily on intensive punitive enforcement efforts such as surveillance, investigations, arrests, and intensified prosecutions. Also, the social services offered tend to be very thin, involving some counseling and recreational opportunities but rarely access to actual jobs or advanced educational placements. While some youth are able to get GEDs or access social programs, very few wind up with jobs, much less well-paying or stable ones.

[51] NYPD. "NYPD Expands Juvenile Crime Reduction Program." NYPD July 2, 2009. http://www.nyc.gov/html/nypd/html/pr/pr_2009_023.shtml
[52] J. David Goodman. "Report Finds Juvenile Program Failed to Reduce Robberies, but Police Are Expanding It." New York Times. January 4, 2016. https://www.nytimes.com/2016/01/05/nyregion/report-finds-juvenile-program-failed-to-reduce-robberies-but-police-are-expanding-it.html
[53] Abigail Kramer. "Ceasefire: The NYPD Zeroes in on Violent Crime." City & State. May 1, 2015. https://www.cityandstateny.com/articles/politics/new-york-city/ceasefire-the-nypd-zeroes-in-on-violent-crime.html
[54] New York City. "Mayor de Blasio and State Courts Announce "Project Fast Track" to Ensure Shooters are Quickly Apprehended and Remain off the Streets." New York City. January 12, 2016. https://www1.nyc.gov/office-of-the-mayor/news/044-16/mayor-de-blasio-state-courts-project-fast-track-ensure-shooters-quickly#/0
[55] Myles Miller. "A Rare Look Inside the NYPD Unit Tasked with Investigating Gang Shootings." NY1, October 23, 2019. https://www.ny1.com/nyc/all-boroughs/news/2019/03/28/a-rare-look-inside-the-nypd-unit-tasked-with-investigating-gang-shootings

In some cases, social supports focus on a variety of life skills and socialization classes which do nothing to create real opportunities for people and reinforce the ethos of personal responsibility that often ends up blaming the victim for their unemployment and educational failure in a community that tends to be incredibly poor, underserved, segregated, and dangerous.

It is certainly true that violent crime is heavily concentrated among a fairly small population of young people in specific neighborhoods. While it may make more sense to target them than indiscriminately stopping and frisking or arresting and summonsing hundreds of thousands of people who've committed no serious crimes, deterrence programs like Ceasefire present their own set of problems.

Most young people who engage in serious criminality are already living in harsh and dangerous circumstances. They don't need more threats and punishment in their lives – they need stability, positive guidance, and real pathways out of poverty. This requires a long-term commitment to their well-being, not a telephone referral and home visits by the same people who arrest and harass them and their friends on the streets.

PROSECUTOR PROFILE: CYRUS VANCE JR.

Since at least 2012, the local prosecutor perhaps most willing to engage in gang takedowns and "extreme collaboration" with the NYPD has been Manhattan District Attorney Cyrus Vance Jr. In the gang conspiracy cases that accompanied takedowns in West Harlem, Manhattan DA prosecutors worked "hand in glove" with police and prison officials, the culmination of a new model: "intelligence-led prosecution."[56]

In 2010, Vance, not long after being elected, created the Crime Strategies Unit (CSU), which was designed for "rigorous collection of background information about the people, places, and problems driving crime in specific neighborhoods." The CSU program represents what we believe to be the most important prosecutorial model for gang enforcement in New York City and it preceded a new wave of large scale gang raids in 2011 and 2012 in Harlem.

At the program's outset, the Manhattan District Attorney's Office conducted "precinct-based crime assessments" of each Manhattan precinct that mapped out crime "hot spots" and listed out gangs and crews. According to the Manhattan District Attorney's 2018 "Intelligence-Driven Prosecution: Implementation Guide," Manhattan is divided into five areas, each of which is assigned an Assistant District Attorney, an intelligence analyst and a community affairs coordinator. At the same time, Assistant District Attorneys, in collaboration with precinct commanders and NYPD Field Intelligence Officers (FIO), identified at least 25 priority offenders in each precinct, which would amount to over 1,000 offenders at the outset of the program.

According to a 2016 study of the prosecution model by the Center for Court Innovation, CSU staff "can continuously expand the list of priority offenders and/or record relevant intelligence."[57] However, like the NYPD gang database, it is not clear by what process prosecutors make such lists.

[56] Chip Brown. "Cyrus Vance Jr.'s 'Moneyball' Approach to Crime." New York Times Magazine. December 3, 2014. https://www.nytimes.com/2014/12/07/magazine/cyrus-vance-jrs-moneyball-approach-to-crime.html

[57] Jennifer A. Tallon, Dana Kralstein, Erin J. Farley, and Michael Rempel. "The Intelligence-Driven Prosecution Model: A Case Study in the New York County District Attorney's Office." The Center for Court Intervention. 2016. https://www.courtinnovation.org/sites/default/files/documents/IDPM_Research_Report_FINAL.PDF

The CSU is informed by four programs:

- **The Arrest Alert System is a database and "early warning system" of priority offenders whose arrest immediately alerts the CSU and NYPD personnel.**
- **The Surveillance Camera Interactive Map (SCIM) "shows the locations of and contact information for some 6,000 public and private surveillance cameras in Manhattan."**
- **The Crime Prevention System database "which targets violent crimes and gathers on one spreadsheet... details about a defendant, including nicknames, which can be linked to additional information: friends, tattoos, telltale scars, Facebook entries, geo-coded street addresses, debriefing tips, excerpts from jailhouse phone calls."**
- **The InPho program "analyzes recorded inmate phone calls from Rikers Island."**

We believe that the **Crime Prevention System Database** parallels the NYPD gang database. Not only do some of the same details tracked in the database include criteria used in the NYPD gang database (friends, tattoos, scars, social media), the database is searchable by gang, which suggests that the Manhattan District Attorney is either classifying gangs and gang membership on its own or sharing that information with the police department, which the NYPD has said does not happen.

The **Arrest Alert System** is described as the "nerve center" of the CSU and the Office's overall approach to tracking street crime and gangs. In a 2014 New York Times article, then Assistant District Attorney Kerry Chicon said, "We are constantly adding, deleting, editing and updating the intelligence in the Arrest Alert System. If someone gets out of a gang, or goes to prison for a long time, or moves out of the city or the state, or ages out of being a focus for us, or dies, we edit the system accordingly — we do that all the time."[58]

The Arrest Alert System allows for prosecutors and certain police units, like the NYPD Gang Unit, to be alerted through email alerts when certain people are arrested, likely those deemed "priority offenders." When prosecutors are alerted to the arrest of a priority offender, they can draft enhanced bail applications and elevate charges, according to the Center for Court Innovation report. In open cases, prosecutors can alert the judge of an existing case if there is a second arrest.

One of the advantages for prosecutors is being able to collect information on the suspect not available on their rap sheet, like their gang status. As the Center for Court Innovation report notes, CSU staff "can reach out to the ADA writing up the case in the Early Case Assessment Bureau (ECAB) to inform the prosecutor of pertinent information related to the defendant's criminal activity unavailable on the rap sheet (such as whether the defendant is a member of a violent gang)." This not only changes how a prosecutor might handle a case, it has been shown to change outcomes. According to the Center for Court Innovation report, cases impacted by the Arrest Alert System more often set bail, and when they did bail was higher.

Another function of the Arrest Alert System is to develop area-based intelligence on suspected future gang offenders. As the Center for Court Innovation report describes, "arrest alerts helped prosecutors gather intelligence on up and-coming gang members."

Debriefings

An alert from the Arrest Alert System can also notify prosecutors when someone is breaking a curfew or violating a condition of parole. It also creates

[58] Chip Brown. "Cyrus Vance Jr.'s 'Moneyball' Approach to Crime." New York Times Magazine. December 3, 2014. https://www.nytimes.com/2014/12/07/magazine/cyrus-vance-jrs-moneyball-approach-to-crime.html

opportunities for prosecutors to pull suspects into interrogation-like "debriefings." Former ADA Chicon:

"Every morning, I talk to my five A.D.A.s, who are experts in their areas. We decide whom we should try to pull out for a debriefing. We don't debrief people arrested for felonies because we don't want to compromise a case. We pull people arrested on low-level misdemeanor charges, maybe two or three a week. We read them their Miranda rights. About 80 percent of them will talk. If you speak to a 16-year-old, they might tell you, 'This kid is running things, this kid is a hanger-on.'

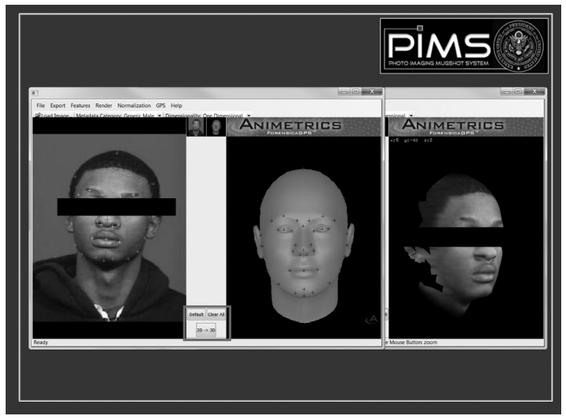
That's how we find out information like whether a gang has changed their name. We took down the Flow Boyz gang at the Robert F. Wagner housing project in 2012. But a lot of those gang members have aged out, and now there's a new group of 14- and 15-year-olds who want their own set name. Through debriefings, we learned they call themselves Only the Wagner."

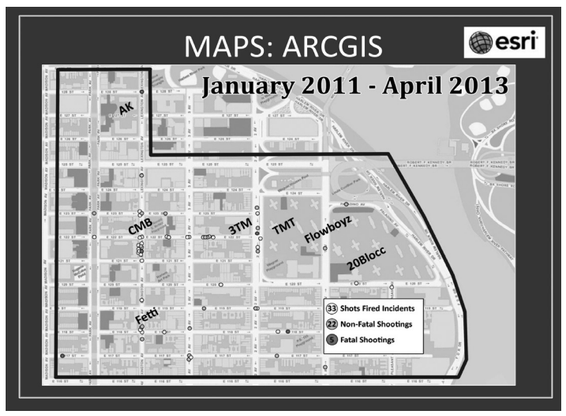
Debriefings are conducted by CSA area prosecutors not to gather additional information or evidence to support the new arrest," according to the Intelligence-led Prosecution handbook. In other words, prosecutors use debriefings to fish for information that could help them score convictions above misdemeanors. In this sense, debriefings can provide an incentive for low-level police harassment and interactions.

When a debriefing is "positive," the handbook explains, a "debriefing memo" is created. Memos are disseminated throughout the office. As cases are built, "photos of defendants associated with geographic hotspots, gangs or specific crime issues are compiled into Microsoft PowerPoint slides which resemble photo arrays - rows of small passport-size photos. Defendants are grouped according to their gang affiliation, geographic area (predominantly a particular housing development hotspot), or other criminal association," the handbook says.

Technology

As one of the most visible and well-resourced prosecutors in the country, the Manhattan DA's Office has become a proponent of using technology. The Photo Imagine Mugshot System (PIMS), which employs facial recognition technology, the ARCGIS map system, which





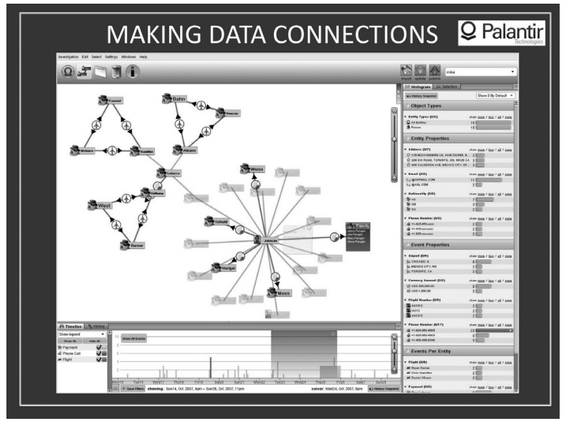
digitally maps out shootings and gang territory, and X-1, which tracks social media posts and direct messages by date(s), time and frequency, are key parts of its Intelligence-led Prosecution model.

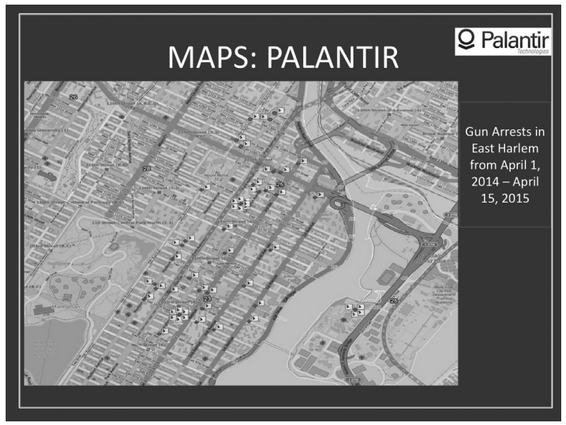
All of those programs are provided by private companies. In-house programs include "DANY311, an application allowing ADAs to submit questions to CSU electronically," as well as the "Glossary of Street Slang," which the report describes as "a system gathering intelligence from sources such as defendant phone calls within city jail."

Perhaps the most notable private software used by Vance's office is Palantir, the California-based data analytics firm that has contracted with the military. Its software has been used by the Manhattan DA to map arrests and make data connections between individuals using addresses, phone numbers and even nationality.

In New York, Palantir technology was reportedly instrumental in helping the NYPD plan a sting operation that led to a gang takedown in Brooklyn that included well-known rapper Bobby Shmurda.[59] According to The Verge, Palantir was also used to construct a controversial "heat list" for the Chicago Police Department using algorithms to predict the most likely violent criminals.[60] It was also uncovered to be part of a secretive "predictive policing" program with the New Orleans Police Department (NOPD) to build racketeering cases against alleged gang members.

New Orleans moved to end their relationship with Palantir partly because local lawmakers didn't even know the city was using the program since it was funded through a philanthropic organization tied to the mayor. In New York, the Manhattan District Attorney's Office,





which has vast amounts of money obtained through asset forfeitures, similarly operates with a budget largely free from basic oversight.

Cyrus Vance Jr.'s office has been involved in some of the largest gang conspiracy sweeps New York City has ever seen. It worked with the police on a large gang conspiracy case in East Harlem in 2012 when over 60 people were indicted just as the NYPD was rolling out Operation Crew Cut. Vance himself was notably boastful after the 2014 West Harlem raid. Other prosecutors may follow

[59] William Alden. "How Bobby Shmurda Got Busted with Help from Silicon Valley." BuzzFeed. July 3, 2017. https://www.buzzfeednews.com/article/williamalden/how-bobby-shmurda-got-busted-with-help-from-silicon-valley

[60] Ali Winston. "Palentir has Secretly been using New Orleans to Test its Predictive Policing Technology." The Verge. February 27, 2018. https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd

in his steps.The Intelligence-led Prosecution model has reportedly been influential to other prosecutor offices around the country, including Philadelphia and Delaware.

For reformers wary of gang takedowns, Vance is perhaps a poster boy for prosecutors that seek convictions and serious prison time out of questionable gang policing tactics.

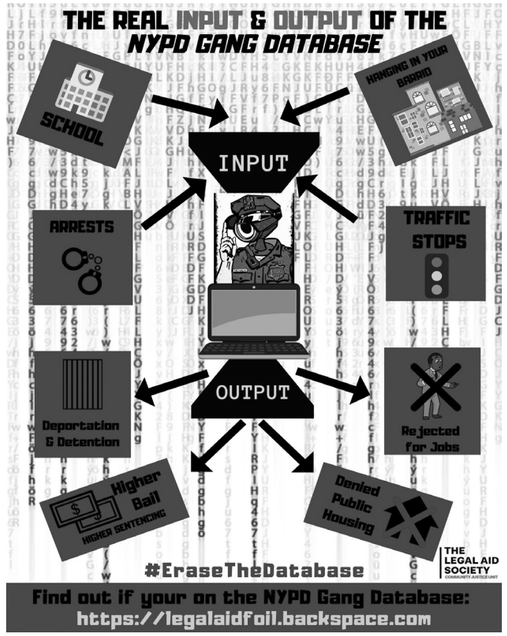
ACTION SPOTLIGHT: LEGAL AID'S FOIL CAMPAIGN

The Community Justice Unit (CJU) of the Legal Aid Society launched the "Do It YourSelf " (D.I.Y.) Freedom of Information Law (FOIL) campaign on February 2018 with the purpose of assisting community members in demanding to know if they had been labeled as gang involved and placed in the NYPD gang database.

Since the police department does not notify individuals about their inclusion into the gang database and there is no requirement of criminality or suspicion of wrongdoing to be placed on it, this further marginalizes communities that are over-policed, depriving them of their right to due process and leaving them without any recourse to challenge that inclusion.

CJU's D.I.Y. FOIL initiative is a way to push back against the black box of secrecy surrounding gang policing by providing community members with a legal tool to demand to know if they have been previously labeled and entered in the gang database.

The CJU launched a website in order to facilitate the D.I.Y. campaign to process FOIL requests more broadly simplifying the process so that people can submit the request directly from their phones or computers.[61] Since launched in 2018, over 350 community members have submitting FOIL requests to the NYPD.



Additionally, CJU has held workshops across New York City with Cure Violence organizations and other community-based organizations raising awareness of the issue and helping people file FOIL requests more broadly; every single request has been outright denied by the police department. This goes against the bedrock principle underlying the Freedom of Information Law, which is supposed to be liberally construed so the public can have maximum access to records of government.

The FOIL initiative has shown that the NYPD is not only comfortable with denying access to every single request, but they are also unwilling to provide records when they have confirmed that they in fact listed the person in their database.

Through the efforts of the FOIL campaign, Legal Aid has also been able to move forward with an Article 78 lawsuit against the NYPD for their failure to disclose records that they had confirmed existed.[62] They are still in the litigation stage of this case as the NYPD continues to use delay tactics in producing the documents that were requested.

[61] The Legal Aid Society Community Justice Unit. "Are You in the Gang Database?" https://foil.backspace.com/

CONCLUSION/RECOMMENDATIONS

Gang policing replicates the harms of mass incarceration strategies that have come under increased scrutiny. It is dangerous and discriminatory and will not uplift neighborhoods struggling with intra-community violence, gang-related or otherwise. Simply put, the approach is racist policing at its worst.

Efforts to push back against gang databases and gang policing, however, should acknowledge that the presence of gangs, though overstated and demonized by the police and the media, is real. Activists and advocates should not only fight for the rights of those mislabeled or completely "innocent," but also for those who may be legitimately connected to gangs or crews.

This report concludes that New York City needs to invest in its residents, gang-affiliated or otherwise, instead of criminalizing them. In order to do that, policy-makers need to acknowledge that cities like New York City are failing to address issues of poverty central to violence. Consider that the US is more segregated today than at any time and that the US allows up to 25% of its young people to grow up in extreme poverty. It is from poverty that the vast majority of serious crime originates.

It is important to understand that we cannot have a dual approach of enforcement and investment because gang policing exacerbates these problems, impacting people's ability to find employment and housing. While local officials sometimes talk about getting to the root causes of gang violence, oftentimes these efforts consist of educational programs run by police and prosecutors that tell young people to avoid gangs without providing them credible alternatives for navigating a hostile environment.

Many young people turn to life on the streets because of problems at home. Their parents are overwhelmed by poverty and the problems that often go with it, such as unstable housing, substance abuse, hunger, and mental illness. Instead of gang takedowns, the city could support parents so that they can better support their children by looking at the structure of working hours and the high costs of childcare as well as direct financial support of families that has been undermined by welfare reforms over the last 30 years.[63]

Still, with more support services in place, the number one challenge young people face is access to stable incomes – even while in school. Expansion of summer employment is an important part of that, but young people also need jobs during the school year to deal with personal and family expenses. Many young people involved in violence also suffer from unstable housing and homelessness. While increased income can help, increases in the stock of truly affordable and public housing (as opposed to banning so-called offenders from housing) is also essential to creating stability for young people.

In schools, education officials need to replace SROs with counselors, restorative justice programs and resources to help students navigate home lives and communities that may be severely disordered and dangerous. Using teachers and SROs to inform on them and criminalize them will serve to undermine their attachment to schooling and drive them out onto the streets, towards violence and/or into the criminal justice system.

One of the primary predictors of violence is past trauma. Youth and adult-aged people involved in violence have

[62] Alice Speri. "NYPD Gang Database Can Turn Unsuspecting New Yorkers into Instant Felons." The Intercept. December 5, 2018. https://theintercept.com/2018/12/05/nypd-gang-database/
[63] Elizabeth Palley and Corey S. Shdaimah. In Our Hands: The Struggle for U.S. Childcare Policy. New York: NYU Press, 2014.

almost always been the victims of violence either in the community or at home. Even when they may not have personally been the victim, they have witnessed the victimization of friends and family members, often repeatedly. The city should provide services to deal with trauma – including mental health and substance abuse services as well as improved educational and recreational services.

New York City has created a new emergency trauma response capability called Mobile Trauma Units that can respond to shootings and provide immediate interventions and referrals to on-going care as available. But there is a lack of adequate services to refer people to, so that capacity must be expanded. These services need to be culturally appropriate and linked to wrap around health and social services support for young people and their families.Those who have experienced trauma and other adverse childhood experiences (ACEs) are also more likely to have substance abuse and mental health challenges. So, in addition to trauma services, they and their families need access to high quality mental health and substance abuse services on demand.

The city already supports programs designed to reduce shootings and violence by relying on community-based "violence interrupters" or "credible messengers" who work with young people. These "messengers" come from the neighborhoods where violence is a problem and have a reputation on the streets that makes them appropriate for peer to peer outreach, mentoring, and counseling designed to break the cycle of violence.[64] These programs operate on the understanding that violence can operate like a disease, spreading from one victim to another.

The John Jay College of Criminal Justice reported that neighborhoods with credible messenger programs had significant crime reductions compared with similar control areas without them. In the East New York site run by the anti-violence community group Man Up!, gun injury rates fell by 50 percent over four years; the control site in East Flatbush fell by only 5 percent. Similarly, shootings were down by 63 percent in the Save Our Streets South Bronx area, but only 17 percent in the East Harlem control neighborhood. New York City should expand the number of credible messenger programs and equip them with more resources to help young people and their families.[65]

Rather than vilifying and criminalizing "gangs" we should include young people and the groups they form into the community process in ways that don't force them to renounce the close connections they form with others in the community. This can be done through "social inclusion" strategies that give these social groupings a legitimate voice in shaping the affairs of their communities and the city. Recent work in Latin America by John Jay College's David Brotherton has shown that these strategies can substantially reduce violence rates.[66]

Gang suppression policing breaks bonds and sows distrust and resentment, especially for young people. Policing and incarceration may actually serve to strengthen gangs, as police officials themselves have conceded. In 2015, the head of the NYPD Gang Division, Kevin Catalina, acknowledged that putting people in Rikers island helped gangs "consolidate" their power: "As a result of, again, jail culture, a lot of them have developed now, not only the crew affiliations that they had, that they developed in the 2000s, but now overall gang affiliations that they picked up while they were inside."[67]

Using police to solve the problems of young people is a misguided strategy. We need to defund police-led interventions and reinvest that money in the kinds of services that will create healthier and more resilient individuals, families and communities.

RECOMMENDED STEPS TO END THE ABUSES OF GANG POLICING:

1. **Stop criminalizing people as "gang members"**
2. **Abolish the NYPD's gang unit**
3. **Abolish gang databases (of any kind)**
4. **Discontinue all "focused deterrence" and other "precision policing" initiatives.**
5. **Stop using large scale "gang takedowns," including the utilization of state and federal conspiracy charges**
6. **Enable protections for immigrants from criminalization and deportation through gang allegations**
7. **End the use of social media monitoring and other forms of digital surveillance**
8. **Invest in additional credible messenger programs and expand resources for gang-involved people**
9. **Divest from policing and instead invest in increased public health programs, sustainable housing, employment development, schools, conflict transformation and alternative accountability models like restorative justice.**
10. **Investigate and audit current gang suppression practices by the NYPD as well as collaboration with local and federal prosecutors**

[64] The Credible Messenger Justice Center. https://cmjcenter.org/
[65] Sheyla A. Delgado, Laila Alsabahi, Kevin Wolff, Nicole Alexander, Patricia Cobar, and Jeffrey A. Butts. "The Effects of Cure Violence in the South Bronx and East New York, Brooklyn." John Jay College Research and Evaluation Center. October 2017.
[66] David Brotherton and Rafael Gude. "Social Inclusion from Below: The Perspectives of Street Gangs and Their Possible Effects on Declining Homicide Rates in Ecuador." Inter-American Development Bank. March 2018.
[67] Rosa Goldensohn. "Gangs to Blame for Brooklyn Shootings, Police Say." DNAinfo. September 27, 2015. https://www.dnainfo.com/new-york/20150927/bed-stuy/rikers-hardened-youth-gangs-blame-for-brooklyn-shootings-police-say/

Name: Jade Magnus Ogunnaike
File Number: Int. No. 487
File Name: Creating comprehensive reporting and oversight of NYPD surveillance technologies
Position: Support

Dear Mister Speaker,

I am Jade Magnus Ogunnaike, and this written testimony is submitted on behalf of Color Of Change, the nation's largest online racial justice organization, which has more than 1.7 million members. We are deeply concerned with the long-unmet need for oversight of New York Police Department (NYPD) surveillance practices, particularly the use and deployment of new and highly-invasive technologies. In 2018, Council Member Vanessa L. Gibson introduced the Public Oversight of Surveillance Technology (POST) Act, which requires the NYPD to disclose how it utilizes electronic surveillance tools.[1] We are calling on you to continue to support Int. No. 487, also known as the POST Act, as it protects our civil rights and prevents unnecessary interactions with the police which often have traumatic, or even deadly consequences.

NYPD surveillance tools present a danger to all New Yorkers, more specifically Black New Yorkers. The NYPD's arsenal of spy tools, at its core, is a flawed form of surveillance that comes at the expense of basic human rights, security, and privacy. It has been scientifically proven that facial recognition technology, which is often used by the NYPD, is inaccurate and miscategorizes the faces of women and Black people.[2] In a test recently conducted by the American Civil Liberties Union, the facial recognition technology known as Rekognition, which is used by Amazon on the general public, incorrectly matched the photos of 28 members of Congress with mug shots of individuals with previous arrests. Alarmingly, these false matches also disproportionately identified six members of the Congressional Black Caucus.[3] It is clear that regulation is needed for this technology.

Along with the proven ways these tools are inaccurate, the growing use of surveillance technology threatens to obscure racial inequalities under the guise of unbiased computer systems. With no oversight of facial recognition technology, Black and Brown people are more likely to have their images saved and run through these databases. Too often, these systems create a risk of information sharing with federal agencies, including Immigration and Customs Enforcement ("ICE"), resulting in arrests, prosecutions, and deportations due to inaccurate identification.

Unregulated surveillance technology uses algorithms to replicate the racial bias in policing that has had life-threatening consequences for our communities. This invasive technology is racist and inaccurate and reinforces a system of oppression that surveils and targets Black people on

[1] "The New York City Council Black, Latino, And Asian Caucus," Press Release, November 28, 2018, https://www.brennancenter.org/sites/default/files/analysis/BLAC%20Endorses%20Post%20Act.pdf.
[2] Steve Lohr, "Facial Recognition Is Accurate, if You're a White Guy," *New York Times*, February 9, 2018, https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.
[3] Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots," *ACLU*, July 26, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

baseless grounds, while also demonizing our physical appearance.[4] With police violence against Black people at an all-time high, allowing the continued unregulated use of NYPD surveillance tools will result in increased and potentially violent interactions with the police.

Your support of Int. No. 487 will greatly benefit Black people, and help to make our communities safer. Thank you for hearing our concerns. If you wish to speak in greater detail, please contact our Campaign Director, Amanda Jackson at amanda.jackson@colorofchange.org to schedule time for us to speak. We hope to see you champion Int. No. 0487 and show your support for the protection of Black people in your jurisdiction and throughout the City of New York.

Sincerely,

Jade Magnus Ogunnaike
Senior Campaign Director
Color Of Change

[4] Teresa Wiltz, "Facial Recognition Software Prompts Privacy, Racism Concerns in Cities and States," *Pew Charitable Trusts*, August 9, 2019, https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2019/08/09/facial-recognition-software-prompts-privacy-racism-concerns-in-cities-and-states.

Council on American-Islamic Relations- New York
46-01 20th Avenue Astoria, New York 11105
www.cair-ny.org | (646) 665-7599
info@ny.cair.com

STATEMENT OF
AHMED MOHAMED ESQ.,
LITIGATION DIRECTOR
COUNCIL ON AMERICAN- ISLAMIC RELATIONS, NEW YORK, INC.

BEFORE THE
COMMITTEE ON PUBLIC SAFTEY
NEW YORK CITY COUNCIL

FOR A HEARING CONCERNING,
CREATING COMPREHENSIVE REPORTING AND OVERSIGHT OF THE NYPD SURVEILLANCE TECHNOLOGIES

PRESENTED
December 18, 2019

Good afternoon, my name is Ahmed Mohamed, and I am the litigation director of the Council of American-Islamic Relations, the New York Chapter ("CAIR-NY"). CAIR-NY is a leading civil rights advocacy group that represents the Muslim community in New York City and across the state.

As an organization that strives to protect the civil liberties of Muslim Americans from discrimination, harassment, hate crimes and more, the Public Oversight of Surveillance Technology Act ("POST Act") is a pivotal step forward for our community and the entire city. The POST Act will strengthen police oversight, promote public safety and transparency, and most importantly safeguard New Yorkers' privacy rights.

Historically, the New York City Police Department ("NYPD") has deployed novel and highly invasive military-grade technologies collecting data on and to track innocent New Yorkers, circumventing democratic oversight and accountability. The capabilities of these tools go far beyond the mind can imagine. Unfortunately, as civilians of New York City we, and our City Council have no clarity or access to understanding the tools the NYPD has accumulated over the years, due to the lack of transparency and supervision in the system.

Some of the tools that we have been able to gather information on consist of but are not limited to: "Stingrays" or cell site simulators that not only spy on the target of the investigation, but also on an untold number of bystanders.[1] Stingrays can "locate and track individuals" as they enter and exit public and private spaces, including locations that would normally require a warrant to search.[2] The NYPD also utilizes mobile X-Ray vans that use radiation to create high resolution images of the interiors of our homes or cars without having to obtain a search warrant.[3] The NYPD has also implemented the use of Automated License Plate Readers ("ALPRs") as part of their surveillance arsenal. ALPRs are often attached to police vehicles or installed on poles. In addition to capturing license plate information, ALPRs also photograph the passengers and drivers in the vehicles. This information has been utilized to profile Muslim Americans who would attend prayers at mosques.[4] Last year, the NYPD announced it was deploying surveillance drones capable of being equipped with facial recognition programming and/or GPS trackers.[5] Without proper oversight and supervision, these tools can engage in questionable and unconstitutional methods of spying and the breach of privacy.

---

[1] Joseph Goldstein, *New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says,* N.Y. TIMES, Feb. 11, 2016, https://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html

[2] Angel Diaz, New York City Police Department Surveillance Technology, Brennan Center for Justice, Oct. 4, 2019, https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology

[3] Conor Friedersdorf, *The NYPD Is Using Mobile X-Ray Vans to Spy on Unknown Targets,* N.Y. ATLANTIC, Oct. 19, 2015, https://www.theatlantic.com/politics/archive/2015/10/the-nypd-is-using-mobile-x-rays-to-spy-on-unknown-targets/411181/

[4] Adam Goldman and Matt Apuzzo, *With cameras, informants, NYPD eyed mosques,* N.Y. THE ASSOCIATED PRESS, Feb. 23, 2012, https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques

[5] Ashley Southall and Ali Winston, "New York Police Say They Will Deploy 14 Drones," The New York Times, December 4, 2018, https://www.nytimes.com/2018/12/04/nyregion/nypd-drones.html.

The invasive data collected from these technologies is integrated by the Domain Awareness System which can be used to track an individual and predict their behavior.[6] The POST Act would reform these abuses offering protection to all New Yorkers, but particularly the community CAIR-NY represents, Muslim Americans. New York City has generally been a diverse hub of cultures, races, religions, and communities. The NYPD has been profiling innocent civilians based on their religion, race, and ethnicity for decades. Since at least 2002, this profiling has disproportionately impacted Muslim Americans in New York City and beyond.[7] According to the Office of Inspector General for the NYPD, although Muslim Americans make up only 3% of New York City's population, 95% of NYPD's political and religious investigations target Muslim New Yorkers and organizations.[8] One reason why the POST Act is so crucial is that many of the most invasive NYPD programs have never produced a single lead let alone stopped a terrorist act.[9] Yet, these same tactics and technologies whose rewards are so tenuous have a very clear cost.

Many Muslim Americans have been the victims of extensive and suspicionless surveillance for years, suffering from secondhand citizen treatment. NYPD officials have also conducted blanket surveillance of mosques, local businesses owned by Muslims or catering to customers of Middle Eastern descent, and Muslim Student Associations. The NYPD's surveillance of Muslims has had a massive impact and toll on the Muslim community and has created a high level of distrust of law enforcement. Many constituents self-censor and refrain from attending religious gatherings or affiliations. Although most Muslim New Yorkers continue to unapologetically practice their faith in the face of police harassment, some have stopped attending their places of worship. Those who continue to attend mosques face frequent barriers in building trust with fellow community members, fearing them to be undercover officers.[10] Other New Yorkers are afraid to practice their faith as they would wish, refraining from growing a beard, wearing a headscarf or other visible signs of their faith. Muslim faith leaders often speak guardedly to their congregations, fearful that an out of context statement or even a disfavored dialect might spark an investigation.

---

[6] Mariko Hirose, Documents Uncover NYPD's Vast License Plate Reader Database, N.Y. ACLU, Jan. 25, 2016, https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-reader-database

[7] "Factsheet: The NYPD Muslim Surveillance Program." American Civil Liberties Union, https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program

[8] OFFICE OF THE INSEPCTOR GEN. FOR THE N.Y. POLICE DEPT, N.Y. CITY CEPT OF INVESTIGATION, AN INVESTIGATION OF NYPD'S COMPLIANCE WITH RULE GOVERNING INVESTIGATIONS OF POLITICAL ACTVITY (2016), https://www1.nyc.gov/assets/oignypd/downloads/pdf/oig_intel_report_823_final_for_release.pdf

[9] Adam Goldman and Matt Apuzzo, *NYPD: Muslim spying led to no leads, terror cases,* N.Y. THE ASSOCIATED PRESS, Aug. 21, 2012, https://www.ap.org/ap-in-the-news/2012/nypd-muslim-spying-led-to-no-leads-terror-cases

[10] Diala Shamas & Nermeen Arastu, Muslim American Civil Liberties Coalition, Creating Law Enforcement Accountability & Responsibility Project, and Asian American Legal Defense Education Fund. Mapping Muslims: NYPD Spying and Its Impact on American Muslims. Long Island City, NY: Muslim American Civil Liberties Coalition (MACLC): Creating Law Enforcement Accountability & Responsibility (CLEAR) Project: Asian American Legal Defense and Education Fund (AALDEF), 2013.

Research has shown that government surveillance leads to heightened levels of stress, fatigue and anxiety, fosters distrust, and reduces our sense of personal control.[11] Humans are social creatures, and we depend on feeling free to interact with other humans for our health and happiness. Limiting the social, interactive component of a person's life will have an undeniably negative effect on their mental health. In addition, a fear of being watched and monitored, usually without being given an explanation as to why, will impact a person's ability to live their life in an ordinary, healthy way. It will curtail their autonomy to make everyday choices, such as who to speak to or where to go, without fear of adverse repercussions.

After engaging in constant discrimination and unlawful surveillance, the NYPD has earned the distrust of Muslim New Yorkers and other marginalized communities. The NYPD has engaged in unlawful surveillance for over 100 years and the Muslim community is just the latest target. Without proper oversight and supervision, the NYPD will not regain the trust of Muslim New Yorkers. The POST Act does not limit the type of surveillance tools that the NYPD may use. However, the POST Act is a first step in providing transparency and oversight into what surveillance technology the NYPD is hiding from the public and what policies are in place to protect the enormous data they are collecting on us. Other major cities across the nation such as Sommerville, Oakland, Berkeley and San Francisco have adopted significantly more powerful bills and banned certain surveillance technology without having to sacrifice their safety and security.[12] Even the Federal Bureau of Investigation ("FBI") and Department of Justice ("DOJ") have adopted and publicly disclosed their policies for use of certain surveillance technology.[13]

No government entity is above accountable. Sunlight is the best of disinfectants.[14] In simpler terms, sunlight or transparency in the NYPD is the only way to restore faith in the system. As we sit here today, the NYPD has stifled all forms of transparency, including routine Freedom of Information Law ("FOIL") requests. The POST Act only requires the NYPD to disclose basic information regarding the surveillance tools they purchase accompanied with their policies and potential impacts. The NYPD is an entity of the City with a statement mission to improve the "quality of life in New York City by working in partnership with the community to enforce the law, preserve peace, protect the people, reduce fear, and maintain order." We urge the NYPD to follow its mission statement and work with the communities it allegedly serves instead of spying on us. The public and City Council have a right to know what policies are in place for the use of highly invasive surveillance technology. The NYPD's intense pushback on a bill that is designed to bring transparency begs the question: What is the NYPD hiding?

It is this Council's right to mandate transparency; your constituents deserve transparency. We ask that you pass the POST Act without delay.

---

[11] Chris Hawley, *NYPD monitored Muslim Students all over Northeast,* N.Y. THE ASSOCIATED PRESS, Feb. 18, 2012 https://www.ap.org/ap-in-the-news/2012/nypd-monitored-muslim-students-all-over-northeast

[12] Haley Samsel, *Berkeley Becomes Fourth U.S. City to Ban Police Use of Facial Recognition,* SECURITY TODAY, Oct. 18, 2019, https://securitytoday.com/articles/2019/10/18/berkeley-becomes-fourth-city-to-ban-police-use-of-facial-recognition.aspx

[13] Department of Justice, Office of Public Affairs, DOJ Cell-Site Simulator Policy, 9-3-15; https://www.justice.gov/opa/file/767321/download

[14] Brandeis, Louis Dembitz, and Urofsky, Melvin I. Other People's Money and How the Bankers Use It. Bedford Series in History and Culture. Boston: Bedford Books of St. Martin's Press, 1995.

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 487 Res. No. _____

☐ in favor ☒ in opposition

Date: 12-18-19

(PLEASE PRINT)

Name: Deputy Commissioner John Miller

Address: _____

I represent: NYPD

Address: 1 Police Plaza NY, NY 10038

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 487 Res. No. _____

☐ in favor ☒ in opposition

Date: 12-18-19

(PLEASE PRINT)

Name: Assistant Deputy Commissioner OLEG Chernyavsky

Address: _____

I represent: NYPD

Address: 1 Police Plaza, NY NY 10038

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: 12/18/19

(PLEASE PRINT)

Name: Alice Fontier

Address: 360 E. 161st St Bronx NY 10451

I represent: The Bronx Defenders

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: Dec 18th

(PLEASE PRINT)

Name: Sergio De La Pava

Address: _____

I represent: New York County Defender Services

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 482 Res. No. _____

☒ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Elizabeth Daniel Vasquez

Address: _____

I represent: Brooklyn Defender Services

Address: 177 Livingston Street, Brooklyn

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

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

☑ in favor ☐ in opposition

Date: 12/18/19

(PLEASE PRINT)

Name: Alex Yilab

Address: _____

I represent: Brooklyn College

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. 487-2018 Res. No. _____

☐ in favor ☐ in opposition

Date: DEC. 18, 2019

(PLEASE PRINT)

Name: BARRY FRIEDMAN

Address: SUITE 302, NYU SCHOOL OF LAW, 40 WASHINGTON SQ. S
NEW YORK, NY 10012

I represent: THE POLICING PROJECT AT NYU LAW

Address: SUITE 302, NYU SCHOOL OF LAW, 40 WASHINGTON SQ. S.

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: 12/18/19

(PLEASE PRINT)

Name: Towaki Komatsu

Address: Private

I represent: Self

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 487 Res. No. _____

☐ in favor ☐ in opposition

Date: 12/18/19

(PLEASE PRINT)

Name: Michael Sisitzky

Address: _____

I represent: NYCLU

Address: 125 Whitehall Street

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. 487 Res. No. _____

☑ in favor ☐ in opposition

Date: 12/18/19

(PLEASE PRINT)

Name: John Cusick

Address: _____

I represent: NAACP Legal Defense Fund

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Albert Cahn, Jerome Greco panel

Appearance Card

I intend to appear and speak on Int. No. 487 Res. No. _____

☐ in favor ☐ in opposition

Date: 12/19

(PLEASE PRINT)

Name: Angel Diaz

Address: 120 Broadway

I represent: Brennan Center for Justice

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Angel Diaz, Michael Jerome

Appearance Card

I intend to appear and speak on Int. No. 487 Res. No. _____

☒ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Alexa Fox Cahn

Address: _____

I represent: S.T.O.P.

Address: 40 Exchange Pl

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

Panel
Albert Cahn
Angel Diaz

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 487-2018 Res. No. _____
☒ in favor ☐ in opposition

Date: 12/18/19

(PLEASE PRINT)

Name: Jerome Greco

Address: 49 Thomas St., NY, NY 10013

I represent: The Legal Aid Society

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 0487 Res. No. _____
☐ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: DEE MANDIYAN

Address: 520 8th AVENUE

I represent: YOUTH JUSTICE BOARD

Address: 520 8th AVENUE

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 0487 Res. No. _____
☒ in favor ☐ in opposition

Date: Dec 18th, 2019

(PLEASE PRINT)

Name: Genevieve Fried

Address: 237 E 17th St Apt 310 New York, NY 10003

I represent: AI NOW INSTITUTE

Address: 155 6th Ave New York, NY 10013

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. 487 Res. No. _____

☑ in favor ☐ in opposition

Date: 12/18/19

(PLEASE PRINT)

Name: AHMED MOHAMED

Address: [redacted]

I represent: The Council on American-Islamic Relations - NY

Address: 46-01 20th Ave, Queens NY 11105

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 0487-2018 Res. No. _____

☒ in favor ☐ in opposition

Date: December 18, 2019

(PLEASE PRINT)

Name: Ras Omeil Novado Morgan

Address: 956 East 84 Street, BK, NY 11236

I represent: Plaintiff Pro Se in Morgan v. City

Address: 17-CV-6454

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: Joseph Sellman

Address: 1422 3rd Ave

I represent: Black Lives Matter Greater NY

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: 12/18/19

(PLEASE PRINT)

Name: Nathan Sheard

Address: 815 Eddy Street, San Francisco, CA 94109

I represent: Electronic Frontier Foundation

Address: ~~Starrett Sykes~~ 928 Jefferson Ave, Brooklyn, NY

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

THE COUNCIL
THE CITY OF NEW YORK

P1

Appearance Card

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

☐ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Hawk Newsome

Address: 955 Sheridan Ave, #5B Bronx NY 10456

I represent: Black Lives Matter Greater NY

Address: Same as Above

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