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.