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]