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.