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