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

December 18, 2019

NYCLU
ACLU of New York

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

Donna Lieberman
Executive Director

Robin Willner
President

The New York Civil Liberties Union ("NYCLU") respectfully submits the following testimony in support of Intro. 487, the Public Oversight of Surveillance Technology ("POST") Act. The NYCLU, the New York affiliate of the American Civil Liberties Union, is a not-for-profit, non-partisan organization with eight offices throughout the state and more than 180,000 members and supporters. The NYCLU's mission is to promote and protect the fundamental rights, principles, and values embodied in the Bill of Rights of the U.S. Constitution and the New York Constitution.

A core component of our work is protecting New Yorkers' rights to be free from discriminatory and unwarranted surveillance by law enforcement. Left unchecked, police surveillance has the potential to chill the exercise of First Amendment-protected speech and religious worship, intrude on Fourth Amendment-protected privacy rights, and cast entire communities under a cloak of suspicion in contravention of the Fourteenth Amendment's guarantee of equal protection.

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

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

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

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

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

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

NYCLU
ACLU of New York

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

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

---

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

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

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

NYCLU
ACLU of New York

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

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

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

A. Cell-Site Simulators/Stingrays

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

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

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

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

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

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

B. X-ray Vans

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

---

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

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

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

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

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

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

C. Face Surveillance

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

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

---

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

[14] Friedersdorf, *supra* note 12.

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

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

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

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

[19] *Id.*

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

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

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

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

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

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

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

---

[21] Garvie, *supra* note 18.

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

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

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

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

IV. Disclosure is Inevitable

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

---

[23] *Id.*
[24] Ashley Southall & Ali Winston, "New York Police Say They Will Deploy 14 Drones," N.Y. Times, Dec. 4, 2018, https://www.nytimes.com/2018/12/04/nyregion/nypd-drones.html.
[25] Jen Chung, "NYPD Launces Drone Program, NYCLU Warns of Overreach," Gothamist, De. 5, 2018, https://gothamist.com/news/nypd-launches-drone-program-nyclu-warns-of-overreach.
[26] Southall, *supra* note 24.

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

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

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

V. Conclusion

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

---

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