BRENNAN
CENTER
FOR JUSTICE

Written Testimony of Ángel Díaz
Counsel, Liberty & National Security Program
Brennan Center for Justice *at NYU School of Law*
Before the New York City Council
Committee on Public Safety
in Support of Int. 487
December 18, 2019

Good afternoon, Chairman Richards and members of the Committee on Public Safety. My name is Ángel Díaz, and I am Counsel for the Liberty and National Security Program at the Brennan Center for Justice. I want to thank Council Members Vanessa Gibson and Brad Lander for their leadership on this issue. I'd also like to thank the 31 co-sponsors of this legislation for their support and acknowledgement of this overdue transparency measure. Finally, thank you to Chairman Richards for holding this necessary hearing and for inviting the Brennan Center to testify.

The Brennan Center is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. The Liberty and National Security Program seeks to ensure that the country's national security laws and policies remain equal to the task of protecting individual rights, constitutional values, and the rule of law. As part of that work, we actively seek greater transparency and oversight of the NYPD's surveillance tools. While emerging technologies bring opportunities for officers to do their jobs more efficiently, they also raise many issues ranging from hidden biases to the potential for misuse. Without oversight, modern surveillance poses serious risks for the civil rights and civil liberties of those most often affected by policing: communities of color and immigrant communities.

We've seen this play out before. Just last month, former Mayor Bloomberg apologized for his support of the unconstitutional stop-and-frisk program, which heavily targeted black and brown young men. [1] But without oversight of the NYPD's surveillance apparatus, we are deploying a system that can result in a digital stop-and-frisk that will be difficult to detect or redress.[2] This is why we need common

[1] Shane Goldmacher, *Michael Bloomberg Pushed 'Stop-and-Frisk' Policing. Now He's Apologizing*, NEW YORK TIMES, November 17, 2019, https://www.nytimes.com/2019/11/17/us/politics/michael-bloomberg-speech.html.

[2] *See* Angel Diaz, *Oversight of Face Recognition Is Needed to Avoid New Era of 'Digital Stop and Frisk'*, BRENNAN CENTER FOR JUSTICE, May 31, 2019, https://www.brennancenter.org/our-work/analysis-opinion/oversight-face-recognition-needed-avoid-new-era-digital-stop-and-frisk.

sense accountability measures in place, and why the Brennan Center urgently calls for the overdue passage of the POST Act.

When the City Council first debated the POST Act in 2017, it had the opportunity to be a leader—now, it has fallen behind. Cities across the country, including San Francisco,[3] Seattle,[4] and Nashville,[5] have all passed laws to rein in unaccountable surveillance. Each of these laws goes further than would be required under the POST Act. In some jurisdictions, police must obtain City Council approval before they can acquire new surveillance tools;[6] a growing number of cities have even passed outright bans of facial recognition technology.[7] Meanwhile, when this Council asked the Department of Information Technology and Telecommunications whether the NYPD uses facial recognition, the DoITT's representative said they did not know.[8]

The POST Act balances the need for democratic oversight and transparency with the NYPD's need to keep certain operational tactics confidential. A strong local democracy like New York City requires at least a basic level of information about what its local police are doing and how they're doing it. The POST Act asks the NYPD to provide public answers to simple questions: what information is the department collecting, with whom is the department sharing it, and what policies are in place to respect the civil rights and civil liberties of New Yorkers? The legislation does not require the disclosure of operational details that might compromise police investigations or harm public safety.

This requirement would cover technologies such as:

- **Facial Recognition.**[9] Studies of many commercially available products have found unacceptable error rates when analyzing faces that are not white and male.[10]

[3] *See* San Francisco, Cal., Ordinance No. 103-19, Stop Secret Surveillance Ordinance, Administrative Code - Acquisition of Surveillance Technology (adopted May 14, 2019), available at https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A.

[4] *See* Seattle, Wash., Ordinance 125,376, Mun. Code § 14.18.080 (Supp. 2019) (adopted Oct. 5, 2018), available at https://seattle.legistar.com/LegislationDetail.aspx?ID=3380220&GUID=95404B0E-A22D-434E-A123-B3A0448BD6FA&Options=Advanced&Search=.

[5] *See* Nashville, Tenn., Ordinance No. BL2017-646, Metro. Code § 13.08.08 (Supp. 2019) (adopted June 7, 2017), available at https://www.nashville.gov/mc/ordinances/term_2015_2019/bl2017_646.htm.

[6] *See, e.g.*, Oakland, Cal., Ordinance No. 13,489, Mun. Code ch. 9.64 (Supp. 2019) (adopted May 15, 2018), available at: http://www2.oaklandnet.com/oakca1/groups/cityadministrator/documents/standard/oak070617.pdf.

[7] *See, e.g.* Caroline Haskins, *Oakland Becomes Third U.S. City to Ban Facial Recognition*, Motherboard, July 17, 2019, available at https://www.vice.com/en_us/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz.

[8] *See* New York City Council, Transcript of the Minutes of the Committee on Housing and Buildings Jointly with the Committee on Technology and the Committee on Consumer Affairs and Business Licensing, October 7, 2019, at 31, available at https://legistar.council.nyc.gov/View.ashx?M=F&ID=7786281&GUID=CB0ABFB0-CF07-4787-9CE9-142D1E65322F.

[9] *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Center on Privacy & Technology, May 16, 2019, available at https://www.flawedfacedata.com/.

[10] *See e.g.,* Joy Buolamwini and Timnit Gerbu, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. of Machine Learning Res. (2018), available at http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

- **Social Media Monitoring.**[11] A New York court has ordered the NYPD to release unredacted documents relating to how the Department uses Dataminr software to monitor social media.[12] This was in response to a public records request filed by Black Lives Matter activists seeking records about NYPD surveillance of their social media profiles.
- **Automatic License Plate Readers.**[13] NYPD contracts with a company called Vigilant Solutions for access to its massive database of license plate reads.[14] If the NYPD shares information captured from its own license plate readers and shares it with other customers of Vigilant Solutions, it may be unwittingly sharing information about undocumented New Yorkers with ICE.[15]

The information that would be disclosed under the POST Act is essential for effective public oversight and is also too general to be a tool for those who might wish to evade lawful police surveillance. It does not provide any information about how the NYPD uses the technology in connection with specific investigations. It does not disclose where or when it might be used or how someone might avoid it. It also does not make the tools any less effective. For example, wiretaps continue to be an important investigative tool despite widespread knowledge of their existence and a strict legal framework governing their use.

While the NYPD might enjoy a brief advantage while its tools remain secret, their existence eventually comes to light—often with a scandal attached. Even a cursory look at recent news shows why NYPD cannot be trusted to police itself:

- When a surveillance photo is too blurry or otherwise inadequate for facial recognition, the NYPD runs photos of celebrity "lookalikes" or uses photo editing software to change a person's appearance.[16]
- The NYPD secretly collects DNA samples from minors as young as 12 by offering them a soda.[17]

[11] *See* Jessie Gomez, *New York court rules NYPD can't use Glomar to keep surveillance records secret*, MUCKROCK, January 15, 2019, available at https://www.muckrock.com/news/archives/2019/jan/15/nypd-glomar-response/.

[12] *See Millions March NYC v. New York City Police Department*, Index No. 100690/2017, January 14, 2019, available at https://www.documentcloud.org/documents/5684800-Millions-March-Nypd.html#document/p1.

[13] *See Automatic License Plate Readers*, NYCLU, available at https://www.nyclu.org/en/automatic-license-plate-readers.

[14] *See* Anthony Romero, *Documents Uncover NYPD's Vast License Plate Reader Database*, HUFFINGTON POST, January 25, 2017, available at https://www.huffpost.com/entry/documents-uncover-nypds-v_b_9070270.

[15] *See* Russell Brandom, *Exclusive: ICE is about to start tracking license plates across the US*, VERGE, January 26, 2018, available at https://www.theverge.com/2018/1/26/16932350/ice-immigration-customs-license-plate-recognition-contract-vigilant-solutions.

[16] *See* Garvie, *Garbage In, Garbage Out*, *supra* note 9.

[17] Jan Random and Ashley Southall, *N.Y.P.D. Detectives Gave a Boy, 12, a Soda. He Landed in a DNA Database*, NEW YORK TIMES, August 15, 2019, available at https://www.nytimes.com/2019/08/15/nyregion/nypd-dna-database.html.

- As of 2018, over 98% of the entries in the NYPD's gang database were listed as either Black or Hispanic.[18]

Earlier this year, the Brennan Center published a chart that tracks each of the NYPD's known surveillance tools based on publicly available information.[19] This chart tracks many of the features included in the POST Act: it describes how each tool works, outlines concerns, and analyzes NYPD policies to the extent they exist. But this report relies on public records requests and advocacy by journalists and lawyers, a costly and slow process offering limited and delayed public access to information.

For example, the Brennan Center was party to a multi-year legal dispute with the NYPD to obtain information about the Department's use of predictive policing technologies. These systems rely on algorithms to analyze large data sets and generate statistical estimates about crime. The estimates are then used to direct police resources.

But predictive policing tools have been roundly criticized by civil rights and civil liberties advocates,[20] as they often rely on historic crime data that can be expected to both reflect and recreate decades of biased enforcement against communities of color.[21] Here in New York, historic crime data might be tainted by the Department's unconstitutional stop-and-frisk program.[22] Relying on this data to inform how police officers are deployed in the future is likely to result in the same biased policing.

These concerns motivated our decision to file a public records request seeking information about the NYPD's testing, development, and use of predictive policing. After the NYPD refused to produce documents in response to our initial public records request and a subsequent appeal, we sued. A little over a year later, we received an order from the court ordering the police department to produce many of the records we had originally requested.[23] Even then, it took almost a full year from the judge's

[18] Josmar Trujillo and Alex S. Vitale, *Gang Takedowns in the de Blasio Era: The Dangers of "Precision Policing,"* POLICING AND SOCIAL JUSTICE PROJECT AT BROOKLYN COLLEGE (2019), at 6, available at https://static1.squarespace.com/static/5de981188ae1bf14a94410f5/t/5df14904887d561d6cc9455e/1576093963895/2019+New+York+City+Gang+Policing+Report+-+FINAL%29.pdf.

[19] Angel Diaz, *New York City Police Department Surveillance Technology*, BRENNAN CENTER FOR JUSTICE, October 4, 2019, available at https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology.

[20] *See, e.g.*, Leadership Conference on Civil and Human Rights, et al., *Predictive Policing Today: A Shared Statement of Civil Rights Concerns* August 31, 2016, available at http://civilrightsdocs.info/pdf/FINAL_JointStatementPredictivePolicing.pdf.

[21] *See, e.g.*, Jack Smith IV, *(Exclusive) Crime-Prediction Tool PredPol Amplifies Racially Biased Policing, Study Shows*, MIC, October 9, 2016, available at https://www.mic.com/articles/156286/crime-prediction-tool-pred-pol-only-amplifies-racially-biased-policing-study-shows. *See also* Laura Nahmias and Miranda Neubauer, *NYPD Testing Crime-Forecast Software*, POLITICO, July 8, 2015, available at https://www.politico.com/states/new-york/city-hall/story/2015/07/nypd-testing-crime-forecast-software-090820 (quoting maker of predictive policing software as noting the importance of assessing "how we apply statistics and data in a way that's going to be sensitive to civil rights and surveillance and privacy concerns").

[22] *See e.g.*, Benjamin Mueller, *New York Police Dept. Agrees to Curb Stop-and-Frisk Tactics*, NEW YORK TIMES, February 2, 2017, available at https://www.nytimes.com/2017/02/02/nyregion/new-york-police-dept-stop-and-frisk.html.

[23] *See* Rachel Levinson-Waldman and Erica Posey, *Court: Public Deserves to Know How NYPD Uses Predictive Policing Software*, BRENNAN CENTER FOR JUSTICE, January 28, 2018, available at https://www.brennancenter.org/blog/court-rejects-nypd-attempts-shield-predictive-policing-disclosure.

order before the NYPD finally produced some of the information in our request. While the documents we ultimately received helped to shed light on the NYPD's predictive policing system, we still do not have a full understanding of how it works.

The goal of the POST Act is to front-load oversight. The bill allows policymakers and community members to have an informed conversation about the rules of the road *before* the NYPD deploys a new technology and before another alarming headline about police surveillance. It also encourages the NYPD to be thoughtful in how it approaches new surveillance technologies. This approach can help prevent foreseeable harms to individual rights, strengthen community trust, and avoid wasting scarce resources.

In fact, the NYPD's commitment to secrecy goes beyond even the federal government's approach. The Department of Justice[24] and the Department of Homeland Security (DHS)[25] each published policies regarding their use of Stingrays. These policies require agents to get a warrant before deploying them and documenting privacy protections. DHS also publicly described its use of backscatter x-ray systems for border security; issued Privacy Impact Assessments for its use of facial recognition[26] and license plate readers[27]; and issued guidance for state and local agencies using drones, strongly recommending transparency and public outreach.[28] If federal agencies tasked with protecting our domestic national security can provide this level of transparency, surely the NYPD should do the same.

As noted in the New York Times' endorsement of the POST Act, advances in artificial intelligence make police surveillance "the newest battleground for civil liberties."[29] Unchecked, modern surveillance tools threaten to completely redefine the right to privacy, freedom of speech, and equal protection under the law. These foundational values must be jealously guarded if New York City is to remain a strong local democracy. It is unsustainable and unacceptable for NYPD surveillance to evade

[24] U.S. Department of Justice, Department of Justice Policy Guidance: Use of Cell-site Simulator Technology, September 3, 2015, available at https://www.justice.gov/opa/file/767321/download.

[25] Memorandum from Alejandro N. Mayorkas to Sarah Saldana, et al., *Department Policy Regarding the Use of Cell-Site Simulator Technology*, October 19, 2015, available at https://www.dhs.gov/sites/default/files/publications/Department Policy Regarding the Use of Cell-Site Simulator Technology.pdf.

[26] U.S. Department of Homeland Security, U.S. Customs and Border Protection, *Privacy Impact Assessment for the Facial Recognition Air Entry Pilot*, DHS/CBP/PIA-025, March 11, 2015, available at https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp-1-to-1-facial-recognition-air-entry-pilot-march-11-2015.pdf.

[27] U.S. Department of Homeland Security, U.S. Immigrations and Customs Enforcement, *Privacy Impact Assessment for the Acquisition and Use of License Plate Reader Data from a Commercial Service*, DHS/ICE/PIA-039, March 19, 2015, available at https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-lpr-march2015.pdf.

[28] U.S. Department of Homeland Security, Privacy, Civil Rights & Civil Liberties Unmanned Systems Working Group, *Best Practices for Protecting Privacy, Civil Rights & Civil Liberties in Unmanned Systems Programs*, December 18, 2015, available at https://www.dhs.gov/sites/default/files/publications/UAS%20Best%20Practices.pdf.

[29] New York Times Editorial Board, *San Francisco Banned Facial Recognition. New York Isn't Even Close*, NEW YORK TIMES, May 18, 2019, available at https://www.nytimes.com/2019/05/18/opinion/nypd-post-act-surveillance.html.

accountability any longer. The Brennan Center strongly supports Int. 487 and urges the Council to pass it quickly.

Thank you again for the opportunity to testify. I am happy to answer any questions.