February 24, 2021

Dermot F. Shea
Police Commissioner
New York City Police Department
One Police Plaza, New York, New York 10038

Margaret Garnett
Commissioner of the Department of Investigation
New York City Police Department
180 Maiden Lane, New York, New York 10038

Re: New York City Police Department (NYPD) Impact & Use Policies

Dear Commissioners Shea & Garnett,

The undersigned coalition writes to express concern that the NYPD's draft impact and use policies do not reflect a good faith effort to comply with the requirements of the Public Oversight of Surveillance Technology Act (POST Act).[1] We urge the NYPD to update these disclosures to provide the transparency necessary to enable the public and the City Council to effectively assess the civil rights, civil liberties, and racial justice impacts of the Department's sprawling surveillance system.

The NYPD's pervasive use of technology to track, monitor, and surveil New Yorkers can redefine public spaces, dictate who can enjoy these spaces, and continue to cast an undue level of suspicion and surveillance on communities of color, eroding civil rights and constitutional protections. Without meaningful transparency and effective oversight, the NYPD will continue to conceal its use of surveillance technology, prevent government and the public from studying the impact of these systems, and shield itself from accountability.

I. The draft policies fail to address systemic racial discrimination and other disparate impact concerns.

The POST Act requires the NYPD to address the disparate impacts of each surveillance tool, but the NYPD's draft policies largely provide a simple recitation of civil rights laws and antidiscrimination policies. This fails to consider and mitigate documented instances of technology-facilitated bias as well as disproportionate targeting of communities of color and groups engaging in constitutionally protected activity. For example, the draft policy for the criminal group database, commonly known as the gang database, fails to address the reality that 98.5% of the individuals in the database are nonwhite, with a majority of those individuals coming from Black (66%) and Latinx (31.7%) communities.[2] By comparison, according to the latest survey by the American Community Survey, the overall New York City population is 24.3% Black and 29.2% Latinx.[3] These factors and the lack of validation data create dangerous opportunities for wrongful accusations based on false identifications of individuals through the use of

[1] N.Y.C. Admin. Code § 14-188.

[2] Nick Pinto, "NYPD Added Nearly 2,500 New People to Its Gang Database in the Last Year," *The Intercept*, June 28, 2019, available at: https://theintercept.com/2019/06/28/nypd-gang-database-additions/.

[3] See 2018 American Community Survey 1-Year Estimates, "Demographic and Housing Estimates," New York City and Boroughs, available at: https://www1.nyc.gov/assets/planning/download/pdf/planning-level/nyc-population/acs/dem_2018acs1yr_nyc.pdf.

surveillance tools.[4] Similarly, the NYPD's facial recognition policy does not address how the NYPD will prevent the targeting of activists, such as the high-profile incident involving a civil rights activist with Warriors in the Garden, who appears to have been identified through a combination of social media monitoring and facial recognition.[5]

A meaningful analysis of disparate impact must consider far more than whether a tool is used to *intentionally* target someone on the basis of race. Racial bias and discrimination can present itself at numerous points along the development and use of surveillance technology. The training data, model design, technical validation approaches, and implementation strategies can each produce a disparate impact on the lives of Black and brown communities and other protected groups. An adequate assessment for racially disparate impact must not simply state in a conclusory fashion that "the NYPD prohibits the use of racial and bias-based enforcement actions," the NYPD should disclose a more detailed and robust analysis of the actions made in each step in the development, procurement, and deployment of each of its surveillance technologies. Further, a disparate impact assessment of the NYPD's surveillance technologies must interrogate the social context in which these technologies are deployed. This requires a disparate impact assessment to go beyond mathematical and computational analyses and incorporate the impacts of the technologies on communities most directly affected by NYPD surveillance.

Each impact and use policy should provide sufficient information regarding the methods, assumptions, and approaches used by the NYPD such that policymakers and the public are positioned to exercise democratic oversight. General and rote responses, such as the Unmanned Aircraft Systems (UAS) policy's statement that "the safeguards and audit protocols built into this impact and use policy for [body worn cameras] mitigate the risk of impartial and biased law enforcement," are insufficient.[6] Instead, the NYPD's impact and use policies must also assess how NYPD surveillance technologies can contribute to systems of racial stratification and explicitly state the ways in which the Department will ensure its use of facially neutral technologies will not have a disproportionate impact on communities of color.[7]

II. The draft policies fail to disclose how data is collected, stored, and shared in a way that addresses civil liberties and racial equity concerns.

The draft impact and use policies fail to comply with the POST Act's requirements to disclose how information about New Yorkers is collected, stored, and shared. The NYPD must significantly update each

[4] There are at least three known instances of individuals being falsely arrested based on an incorrect facial recognition match. See, Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *The New York Times*, December 29, 2020, available at: https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html; Natalie O'Neill, "Faulty Facial Recognition Led to His Arrest—Now He's Suing," *Vice*, September 4, 2020, available at: https://www.vice.com/en/article/bv8k8a/faulty-facial-recognition-led-to-his-arrestnow-hes-suing; Kashmir Hill, "Wrongfully Accused by an Algorithm," *The New York Times*, June 24, 2020, available at: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

[5] George Joseph and Jake Offenhartz, "NYPD Used Facial Recognition Technology In Siege of Black Lives Matter Activist's Apartment," *Gothamist*, August 14, 2020, available at: https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment.

[6] NYPD Unmanned Aircraft Systems: Impact & Use Policy, available at https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-act/unmanned-aircraft-systems-nypd-impact-and-use-policy-draft-for-public-comment-01.11.2021.pdf.

[7] See Aziz Z. Huq, "Racial Equity in Algorithmic Criminal Justice," 68 Duke Law Journal 1043-1134 (2019); Laura Moy, "A Taxonomy of Police Technology's Racial Inequity Problems," 2021 University of Illinois Law Review 139-193 (2021).

of its draft policies to adequately address and abate the numerous threats to privacy, civil liberties, and racial equity associated with the Department's surveillance practices.

First, the policies do not adequately disclose the types of information collected by each tool, from images collected for facial recognition analysis[8] to historical location information[9] used to track people's movements across time. The policies similarly fail to establish clear controls to ensure that the sheer volume and scope of NYPD surveillance will not infringe on New Yorkers' privacy rights and civil liberties or make even supposedly "anonymized" or "aggregate[d] information" readily re-identifiable through analysis of their overall data set.

Second, the policies do not uniformly include retention policies for each type of data collected by NYPD surveillance technologies. The establishment of clear and reasonable retention periods is essential for a meaningful analysis of the NYPD's data collection practices, as well as analysis of whether data retention enables long-term tracking that requires a higher level of judicial oversight than the NYPD currently obtains prior to engaging in targeted surveillance.

Moreover, the few instances where information about data retention is disclosed reveals overbreadth. For example, a five-year retention period for license plate reader data does not adequately account for civil liberties concerns.[10] Long-term retention of personal data can create increasingly comprehensive and intrusive portraits of people's movements and their private lives.[11] Similarly, the UAS policy limits NYPD's retention of data and images captured by drone surveillance to 30 days, but then notes that images may be retained indefinitely if they are needed for civil litigation, subpoena production, FOIL requests, or other legal processes—reasons that are nearly always present.[12] At the same time, the long-term retention of inaccurate or outdated information can also raise serious civil rights concerns regarding unwarranted criminalization. An audit of California's statewide gang database, for example, found that inaccurate and outdated information was held for years and used for purposes such as employment-related screenings.[13]

Third, the draft impact and use policies fail to adequately inventory and disclose the external agencies with which the NYPD shares data. A major concern underlying passage of the POST Act was the opaque and unaccountable data sharing with agencies ranging from federal immigration authorities to local housing agencies. But the NYPD's disclosures do not provide an accurate and exhaustive inventory of the various

[8] This information can come from a variety of different surveillance practices, such as social media monitoring, drone surveillance, body camera footage, domain awareness system cameras, and more.

[9] This information can be drawn from a combination of different tools, including license plate readers, cell-site simulators, WiFi geolocation devices, and more.

[10] See NYPD License Plate Readers: Impact & Use Policy, available at: https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-act/license-plate-readers-nypd-impact-and-use-policy-draft-for-public-comment-01.11.2021.pdf.

[11] See Department of Homeland Security, "Privacy Impact Assessment for CBP License Plate Reader Technology," 10 ("[A]LPR data from third party sources may, in the aggregate, reveal information about an individual's travel over time, or provide details about an individual's private life, leading to privacy concerns or implicating constitutionally-protected freedoms."), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp049a-cbplprtechnology-july2020.pdf.

[12] See NYPD Unmanned Aircraft Systems: Impact & Use Policy, available at https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-act/unmanned-aircraft-systems-nypd-impact-and-use-policy-draft-for-public-comment-01.11.2021.pdf.

[13] See Auditor of the State of California, The CalGang Criminal Intelligence System, As The Result of Its Weak Oversight Structure, Contains Questionable Information That May Violate Individuals' Privacy Rights, Sacramento, CA, August 2016, 2, https://www.auditor.ca.gov/pdfs/reports/2015-130.pdf.

agencies that share and receive data from various NYPD surveillance databases. Instead, the NYPD makes boilerplate disclosures across policies, such as its assertion that information is "not shared in furtherance of immigration enforcement."[14] This misleading phrasing does not account for the numerous ways in which federal immigration agencies can obtain information from NYPD surveillance practices. NYPD gang policing, for instance, relies on numerous surveillance technologies and is frequently conducted in partnership with federal agencies including Immigration and Customs Enforcement's Homeland Security Investigations (ICE HSI).[15] Similarly, due to the NYPD's participation in the NYC Joint Terrorism Task Force, much of its surveillance data is being shared with federal law enforcement via the New York State Intelligence Center.[16]

The NYPD's draft impact and use policies also fail to account for the extent to which surveillance technology can facilitate unintentional data sharing. For example, an audit in California found that despite efforts from local police to limit data sharing with ICE, confusing vendor settings had left three different ICE agencies with access to license plate reader data from Marin County Sheriff's Office, frustrating compliance with a California law that places controls on local police cooperation with federal immigration authorities.[17] This example also underscores the nexus that exists between data sharing practices and the potential for surveillance technologies to have disparate impact on protected classes. Data-sharing practices which appear neutral on their face, may in fact have disparate harm on protected classes when shared with agencies that deploy them in sensitive settings such as immigration enforcement or public housing. The NYPD's failure to provide adequate disclosures on the disparate impact of its surveillance tools denies the public the opportunity to assess whether practices similar to Marin County are happening in New York City.

The POST Act requires the NYPD to engage in an inventory of its data sharing practices in a way that allows for informed oversight. The impact and use policies must be updated to specifically list every external agency that receives information from the NYPD, disclose the types of data that is collected and the attendant data retention policy, and to specify the controls in place to protect against misuse or unintentional downstream data sharing with other agencies.

III. The draft policies must end overreliance on boilerplate disclosures, address the interdependence of surveillance tools, and establish meaningful audit processes.

Across the board, the NYPD's draft disclosures recycle the same language across drastically different technologies, at times leading to perplexing assertions. For example, several policies suggest tools such as facial recognition or iris recognition technologies do not use "artificial intelligence" and "machine

[14] See, e.g. NYPD Social Network Analysis Tools Impact & Use Policy, available at: https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-act/social-network-analysis-tools-nypd-impact-and-use-policy-draft-for-public-comment-01.11.2021.pdf.

[15] See, e.g., United States Attorney's Office for the Southern District of New York, "120 Members And Associates Of Two Rival Street Gangs In The Bronx Charged In Federal Court With Racketeering, Narcotics, And Firearms Offenses," April 27, 2016, available at: https://www.justice.gov/usao-sdny/pr/120-members-and-associates-two-rival-street-gangs-bronx-charged-federal-court; see also Babe Howell and Priscilla Bustamante, "Report on the Bronx 120 Mass 'Gang' Prosecution," April 2019, available at: https://static1.squarespace.com/static/5caf6f4fb7c92ca13c9903e3/t/5cf914a3db738b00010598b8/1559827620344/Bronx%2B120%2BReport.pdf.

[16] See Michael Price, "National Security and Local Police," *Brennan Center for Justice*, 2013, available at: https://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPolice_web.pdf.

[17] Auditor of the State of California, Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards for the Data It Collects at page 26.

learning." These assertions are misleading and may be technically inaccurate.[18] Artificial intelligence has no standard definition and is an umbrella term that can refer to a wide range of mathematical and technical methods and approaches. Absent a working definition from the NYPD, there is no way to determine if these statements are accurate and if there is institutional competence about the technical aspects of their technologies.

Similarly, the draft policies uniformly fail to name the specific tools that NYPD deploys, as well as whether a tool is provided by a third-party vendor or developed internally. Some tools may even be jointly developed, such as the NYPD's development of the Domain Awareness System with Microsoft[19] or its development of a defunct video analytics systems with IBM.[20] The identity of the vendor is essential for effective oversight, enabling independent evaluation of the capabilities and biases that may be built into a given system. For example, when researchers and advocates identify problems with a particular vendor, it is necessary to know whether the NYPD uses that vendor to advocate for additional investigation and corrective measures. We urge the NYPD to update their policies to make this basic and foundational disclosure.

Modern surveillance systems not only facilitate data sharing across various government agencies, they also frequently integrate with one another. The draft policies fail to adequately disclose this interdependence, instead discussing the use and impact of NYPD surveillance in isolation. This approach does not consider how data analysis and similar systems necessarily depend upon a variety of information collected via tools ranging from surveillance cameras to social media surveillance. We urge the NYPD to update their policies to disclose the manner in which tools are used in tandem in ways that raise novel privacy and civil rights concerns.

Finally, while some draft impact and use policies mention the possibility of audits, they do not specify schedules, assign responsibility for conducting them, or specify the appropriate methodology or criteria for each examination. Updated disclosures must substantively develop and explain the internal processes utilized to ensure the function and impact of these technologies is appropriately monitored. At times, NYPD systems may need to be updated to facilitate audits. For example, a public records lawsuit with the NYPD revealed that its predictive policing system is not set up to create records of its outputs, an intentional design choice that actively frustrates any attempt to evaluate the effectiveness or disparate impact of this system.[21] It is imperative that the NYPD disclose its auditing processes and procedures so that the public can have confidence that the auditing and validation methods sufficiently scrutinizes potential harms to vulnerable

[18] See, e.g., NYPD Facial Recognition: Impact & Use Policy, available at: https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-act/facial-recognition-nypd-impact-and-use-policy-draft-for-public-comment-01.11.2021.pdf; NYPD Iris Recognition: Impact and Use Policy, available at: https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-act/iris-recognition-nypd-impact-and-use-policy-draft-for-public-comment-01.11.2021.pdf.

[19] See Neal Ungerleider, "NYPD, Microsoft Launch All-Seeing 'Domain Awareness System' With Real-Time CCTV, License Plate Monitoring [Updated]," *Fast Company*, August 08, 2012, available at: https://www.fastcompany.com/3000272/nypd-microsoft-launch-all-seeing-domain-awareness-system-real-time-cctv-license-plate-monito.

[20] See George Joseph and Kenneth Lipp, "IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color," *The Intercept*, September 08, 2018, available at: https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/.

[21] See Affidavit of Lesa Moore, Supreme Court of the State of New York, County of New York, Index No. 160541/2016 at Page 2, available at: https://www.brennancenter.org/sites/default/files/Lesa%20Moore%20Affidavit%20in%20Compliance%20-FINAL%20-%20%28%23%20Legal%209761080%29%20%281%29.pdf.

communities and complies with the POST Act. There are a number of critical decisions that can be made in the technical validation or auditing of a policing system that can either obscure or reveal disparities in protected groups.[22]

* * *

In sum, the NYPD has not appropriately investigated the scope, scale, and impact of its surveillance technologies. The draft impact and use policies are plainly insufficient and require significant and immediate updates to provide the transparency and oversight required by the POST Act.

Sincerely,

AI Now Institute, NYU
Andrew Ferguson, Professor of Law, American University Washington College of Law
Brennan Center for Justice at NYU School of Law
The Bronx Defenders
Electronic Frontier Foundation (EFF)
Electronic Privacy Information Center (EPIC)
GANGS Coalition
The Innocence Project
Legal Aid Society
NAACP Legal Defense and Educational Fund, Inc.
New York Civil Liberties Union
The Policing & Social Justice Project at Brooklyn College
Rashida Richardson, Visiting Scholar, Rutgers Law School
S.T.O.P. – The Surveillance Technology Oversight Project

CC:

New York City Mayor Bill de Blasio
New York City Council Speaker Corey Johnson
New York City Council Majority Leader Laurie Cumbo
New York City Council Public Safety Committee Chair Adrienne E. Adams
New York City Council Member Vanessa Gibson

[22] See e.g. Jeff Larson et. al., "How We Analyzed the COMPASS Recidivism Algorithm," *ProPublica*, May 23, 2016, available at: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm; see also, Hilke Schellmann, "Auditors Are Testing Hiring Algorithms For Bias But There's No Easy Fix," *MIT Technology Review*, February 11, 2021, available at: https://www.technologyreview.com/2021/02/11/1017955/auditors-testing-ai-hiring-algorithms-bias-big-questions-remain/.