

February 25, 2021

NYPD Commissioner Shea
New York Police Department
One Police Plaza
New York, NY 10038
Via Email

Re: S.T.O.P. Comment on NYPD's Draft Manned Aircraft Systems ("MAS") Impact & Use Policy

Dear Commissioner Shea:

The Surveillance Technology Oversight Project ("S.T.O.P.")¹ hereby submits our comment in response to the Draft Manned Aircraft Systems ("MAS") Impact and Use Policy ("Policy") published by the New York City Police Department ("NYPD") on January 11, 2021 pursuant to the Public Oversight of Surveillance Technology Act ("POST Act"). Not only did S.T.O.P. work extensively to promote passage of the POST Act, the law's enactment was one of the reasons we were founded. Sadly, upon review, the Policy is so grossly inadequate that it not only undermines public trust and accountability, it violates the NYPD's reporting obligations under the POST Act.

Instead of publishing an impact statement that tells New Yorkers what surveillance tools the NYPD uses, we were provided copy-and-paste responses that are opaque, misleading, and, at times, blatantly wrong. As written, the Policy primarily tell New Yorkers one thing: the NYPD cannot be trusted to use MAS.

Data Sharing Agreements

The POST Act requires the NYPD to enumerate all entities which are able to access the Department's MAS data. However, instead of providing any meaningful information, the Policy merely states that unspecified "agencies at the local, state, and federal level . . . have limited access to NYPD computer and case management systems." At a minimum, the Department must provide a full accounting of all agencies that access such data, along with the frequency of access and any limitations on how such data is used and retained. The NYPD would also need to provide a copy of any/all agreements with external agencies pertaining to the scope of agency access and the volume of data retained.

Vendors and Product Disclosure

Perhaps no aspect of the Policy is more antithetical to the text and spirit of the POST Act than the Department's systematic failure to specify the make and model of equipment used for MAS. The driving impetus for the POST Act was the Department's historical failure to disclose what tools it

¹ S.T.O.P." is a non-profit organization that advocates and litigates for New Yorkers' privacy rights, fighting discriminatory surveillance. For more information see <https://www.stopspying.org/>.

purchased to monitor New Yorkers until years or decades after the fact. This type of surreptitious procurement is antithetical to democratic government and the role of the City Council in overseeing agency purchases. Rather than comply with the POST Act's reporting obligations, the Policy describes the Department's MAS program in vague, non-descript terms. The Policy fails to include a single vendor name, let alone the comprehensive listing of tools that lawmakers required to be provided. At a minimum, the revised policy must include the name of every single MAS system, including the software associated with the aircraft equipment, employed by the NYPD, the system's manufacturer, and the names of any other vendors involved in creating or operating the system. The NYPD should also provide a comprehensive evaluation of what data is accessed and/or retained by vendors. The Policy clearly states that the NYPD allows vendors access to at least some data from MAS but does not sufficiently explain how much and what kind of data is shared. The Policy's reference to a "least privilege principle" where vendors can only access information on a "need to know basis" is impossibly vague and inadequate.

Racial Ethnic, and Religious Bias

Racial discrimination and bias have defined New York City's policing since before the NYPD was even founded, and that deadly legacy of injustice has continued to this day. The POST Act provided the Department with a unique opportunity to address the ways that its surveillance operations have been driven by, and in turn fueled, discrimination for decades. Sadly, rather than addressing this challenge head on, the Department simply ignored the POST Act's requirements, responding with a terse and unbelievable claim that "The NYPD prohibits the use of racial and bias-based profiling in law enforcement actions." This statement is patently absurd. The NYPD has long been emblematic to the country as a symbol of biased-policing,² and after the Department's violent and discriminatory response to recent protests, it's clear just how little has changed.³ MAS exacerbate officers' bias, discriminating against BIPOC and LGBTQ+ communities, putting over-surveilled New Yorkers at risk of wrongful arrests and worse.

Retention Periods and Access Rights

To meet the minimum transparency requirements set out in the POST Act, NYPD must also clarify how long data is saved and how the access rights to the information is determined. The Policy does not provide sufficiently detailed information about the retention periods of the data collected through MAS. Even though the Policy explains that video footage from MAS gets transmitted to the Lower Manhattan Security Initiative (LMSI), and is deleted permanently after 30 days unless the footage is requested as part of an investigation, the Policy does not give any justification for this retention period. Further, the Policy states that the local retention of footage on the aircraft depends on local storage capacity without providing the average local storage capacity on MAS used by the NYPD. The Department also fails to clearly and coherently describe access rights for NYPD employees and contractors to access this exceptionally sensitive data. Bland phrases stating that access rights are given to personnel with an "articulable need" and that access is "further limited based on lawful duty" are feeble efforts to circumvent the reporting obligations set out in the POST Act.

² Lauren del Valle, *NYPD didn't substantiate any complaints of police bias over 4 years. Report cites need to improve*, CNN (Updated 12:10 PM EDT, Jun. 27, 2019), <https://www.cnn.com/2019/06/27/us/nypd-bias-complaints-report/index.html>.

³ See Julie Ciccolini and Ida Sawyer, "Kettling" Protesters in the Bronx: Systemic Police Brutality and Its Costs in the United States, Human Rights Watch (Sep. 30, 2020), <https://www.hrw.org/report/2020/09/30/kettling-protesters-bronx/systemic-police-brutality-and-its-costs-united-states>.

NYPD Data Security

The NYPD is not just asking New Yorkers to allow the Department access to huge volumes of intimate data about our private lives, they want us to let that data to be accessible to anyone who can break into the NYPD's systems. Sadly, we have no way to judge the risk that this data could fall into the hands of any hacker, criminal, or rogue state that could breach NYPD security measures. That is because the NYPD's data security promises are full of repetitive and empty phrases. The section contains general descriptions about the safeguards in place for the Department's case management and computer systems, stating that NYPD uses a "multifaceted approach to secure data and user accessibility."

Not only is the provided information insufficient to build public trust and accountability, it is also so generic as to be almost completely useless from a technical standpoint. The NYPD references its use of Lightweight Directory Access Protocol, dual factor authentication, Secure Socket Layer, and Transport Layer Security. These rudimentary encryption and security features are so ubiquitous that it would only be notable if they were not used as part of the NYPD's data security policy. This is about as persuasive as arguing that a car is safe simply because it has functioning seatbelts; the real surprise would be finding a car that did not. The enormous amounts of highly sensitive data processed through the NYPD's MAS systems call for higher security standards than what is described in the Policy.

NYPD Training

The Policy recognizes the self-evident truth that training is an important factor for the NYPD's use of MAS. For example, the Policy states that every NYPD employee who gains access to MAS must "be a member in good standing of the NYPD Aviation Unit." The Policy goes on to provide very little detail on the topic of training, including the vague statement that it involves classroom instruction as well as practical training while in flight. It is impossible, without more information, to understand the extent and content of the training that officers must go through to operate this highly complicated surveillance tool.

Comparison of the POST Act to other CCOPS Jurisdictions

The Department's failure to provide the public with meaningful details is particularly egregious in light of the strong national record of compliance with analogous efforts. As of today, more than a dozen localities have adopted Community Control Over Police Surveillance (CCOPS). The POST Act is an outlier, both in that it is one of the weakest laws in the country and because the NYPD's response has shown an unprecedented effort to circumvent even the most minimal transparency requirements.⁴ While many municipalities' legislations require acquisition approval, bans non-disclosure agreements and provide a right of action for private citizens, the POST Act only requires the NYPD to provide annual reports and use policies. Notwithstanding this, NYPD has shown unable to meet the requirements set out in the POST Act, by only providing opaque or boiler-plate responses in the Policy, hiding the details needed for meaningful public engagement.

⁴ Hogan Lovells and Surveillance Technology Oversight Project, *New CCOPS On The Beat* (Feb. 10, 2021), <https://static1.squarespace.com/static/5c1bfc7ee175995a4ceb638/t/602430a5ef89df2ce6894ce1/1612984485653/Ne+w+CCOPS+On+The+Beat.pdf>.

Monitoring Political Rallies

The Policy describes MAS used by NYPD as including helicopters and fixed wing aircraft equipped with video, radar, temperature, location sensor technologies as well as “infrared thermal imaging cameras that measure temperature by capturing different levels of infrared light omitted from all people and objects.” According to the Policy, “the cameras provide an enhanced picture of incident scenes by layering heat signatures of individuals and objects on top of the aerial video simultaneously being recorded.” New Yorkers who observed helicopters flying over BLM protestors during the summer of 2020 have every reason to suspect that the NYPD uses MAS equipped with such intrusive technology for protest surveillance. This is made all the more likely by recent revelations that the federal government recorded protests in 15 cities across the US, including New York, and shared this video footage with local law enforcement agencies.⁵ Despite every reason to believe that the NYPD has used MAS to monitor peaceful protests, the Policy contains no information about whether such surveillance has taken place or is allowed by the Department. To the contrary, the Policy’s false, boilerplate reassurance undermines the very transparency and accountability the POST Act was enacted to support. Importantly, this type of omission may be a violation of the NYPD’s reporting obligations, exposing the Department to civil legal penalties.

Concluding Remarks

The cumulative impact of the forgoing errors and omissions is clear: the NYPD is breaking the law. The POST Act is not a formality, it is not a nicety, it is binding legislation with full force of law. When the NYPD fails to comply with the statute, it seeks to overturn the will of the New York’s elected leaders, accomplishing by force what it failed to do through lobbying. If the NYPD persists in this flagrant disregard for its statutory reporting requirements, it will simply hasten the enactment of far more sweeping changes to the Department’s surveillance powers in the coming months.

Sincerely,

/s/
Albert Fox Cahn, Esq.
Executive Director

⁵ Zolan Kanno-Youngs, U.S. *Watched George Floyd Protests in 15 Cities Using Aerial Surveillance*, N.Y. TIMES (June 19, 2020) <https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html>.