SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (646) 602-5600

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 Cell-Site Simulators 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 Cell-Site Simulators 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 cell-site simulators.

Data Sharing Agreements
The POST Act requires the NYPD to enumerate all entities which are able to access the Department's cell-site simulators data. Instead of providing any meaningful information, the Policy merely states that, "[a]s the NYPD does not record, store, or retain any of the data processed cell-site simulators, there are no policies or procedures relating to retention, access, and use of collected data." However, the Policy states that cell-site simulators are used in conjunction with vendor-provided software, and the Policy must, at the very least, reveal the vendors and contractors that provide the cell-site simulators-related software to the NYPD and address the data sharing policies of these vendors.

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 cell-site simulators. The driving impetus for the POST Act was the Department's historical failure to disclose what tools it purchased to monitor New Yorkers until years or decades after the fact. This type of

[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/.

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 cell-site simulators 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 cell-site simulator system employed by the NYPD, the system's manufacturer, and the names of any other vendors involved in creating or operating the system. As mentioned in the previous section, the NYPD should also provide a comprehensive evaluation of what data is accessed and/or retained by vendors.

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] Cell-site simulators exacerbate biased-policing because they give the NYPD location surveillance powers, which puts over-surveilled New Yorkers, primarily BIPOC and LGBTQ+ 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 clarify what access rights officers have to cell-site simulators. The Policy relies entirely on the safeguards of the probable cause order procedure but contains an exception for exigent circumstances that is not explained in sufficient detail, and the Policy does not provide sufficient information about the number of authorized personnel that will be granted access to the cell-site simulators data once a court order is obtained. The current claim that no data is retained from cell-site simulators is patently false. Not only is this inconsistent with publicly reported details about the operation of cell-site simulators, it ignores the fact that cell-site simulator data has been introduced in prior court cases.

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. The enormous amounts of highly sensitive data processed through the NYPD's cell-site simulator

---

[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.

systems, even if not retained and stored long-term, 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 cell-site simulators. For example, the Policy states that members of NYPD Technical Assistance Response Unit (TARU) who gains access to cell-site simulators must first complete a training in the tool and accompanying software. Sadly, the section of the policy on training is limited to two generic sentences that provide no detailed information about what the required training entails. The Policy's training section is grossly insufficient to say the least.

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. As a result, it is clear that more aggressive legislative responses are required.

Monitoring Political Rallies

The Policy does not address whether the NYPD uses cell-site simulators to identify or monitor people in crowds or at political rallies. However, it states that, "NYPD investigations involving political activity are conducted by the Intelligence Bureau, which is the sole entity in the NYPD that may conduct investigations involving political activity pursuant to the *Handschu* Consent Decree." The fact that the Policy mentions political activity without elaborating on the relevance of it to the use of cell-site simulators is enough to arouse serious suspicions about the technology being used for protest surveillance. The Policy must directly address whether the NYPD uses cell-site simulators for protest surveillance.

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.

---

[4] Hogan Lovells and Surveillance Technology Oversight Project, *New CCOPS On The Beat* (Feb. 10, 2021), https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/602430a5ef89df2ce6894ce1/1612984485653/New+CCOPS+On+The+Beat.pdf.

Sincerely,

/s/_____
Albert Fox Cahn, Esq.
Executive Director