BRENNAN CENTER FOR JUSTICE

February 25, 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) Online Monitoring Policies

Dear Commissioners Shea & Garnett,

The Brennan Center for Justice writes to express concern that the New York City Police Department's (NYPD's) draft policies related to social media and online monitoring do not comply with the requirements of the Public Oversight of Surveillance Technology Act (POST Act).

Social media is a crucial forum for the exchange of ideas, particularly in this time of unprecedented public activism and political engagement. Social media platforms like Facebook, Twitter, and Instagram have proven to be an invaluable tool for connecting and organizing around a variety of issues and across diverse movements. In a time when social media is recognized as the "modern public square,"[1] social media monitoring has significant civil rights implications. Like other forms of surveillance, social media monitoring impacts what people say and whom they interact with online. The detrimental effects of surveillance on free speech have been well documented in empirical research.[2]

[1] Packingham v. North Carolina, 137 S.Ct. 1730, 1737 (2017) (quoting Reno v. American Civil Liberties Union, 521 U.S. 844, 868 (1997)).

[2] *See, e.g.*, Faiza Patel, Rachel Levinson-Waldman, Sophia DenUyl, & Raya Koreh, *Social Media Monitoring*, Brennan Center For Justice, May 22, 2019, https://www.brennancenter.org/publication/social-media-monitoring; Elizabeth Stoycheff et al., "Privacy and the Panopticon: Online Mass Surveillance's Deterrence and Chilling Effects," *New Media & Society* 21 (2018): 1-18.

The use of media aggregation services, social network analysis tools, and internet attribution management infrastructure appear to be essential components of NYPD's social media surveillance practices. However, the NYPD's policies regarding these technologies are so vague and contain so little concrete information that they preclude public accountability. We urge the NYPD to revise these policies to permit an effective assessment of their impact on the civil liberties of all New Yorkers, and especially on communities of color.

Moreover, information obtained from social media surveillance tools often informs or intersects with other systems disclosed in the POST Act impact and use policies – for example, the Department's data analysis tool and the criminal group database (commonly known as the gang database). The NYPD's failure to disclose and assess the interconnectedness of its various surveillance tools is a fundamental shortcoming uniting the draft policies.

I. Media Aggregation Services Policy[3]

Media aggregation services search across thousands of sources of information on the internet and send alerts to the NYPD. The draft impact and use policy on media aggregation services fails to comply with the POST Act's requirement that the NYPD disclose how information about New Yorkers is collected, used, stored, and shared through its use of this technology. The NYPD must revise its policy and specify, beyond the mere recitation of boiler plate language, how officers make use of media aggregation services, who supplies these tools, how their use is subject to adequate oversight, and how the department can mitigate their disparate impact upon communities of color.

First, media aggregation services rely heavily on geolocation data — for example, by allowing police to examine the publicly available content being shared in Times Square, an example the policy specifically contemplates. The NYPD's policy provides little information about how such location data is obtained; while it indicates that an alert may contain "geographic location relevant to the information," it does not reveal how that geographical data will be obtained – whether by extracting and analyzing metadata, reviewing keywords related to location, or other measures.

Second, the draft policy fails to clarify the NYPD's rules, processes, and guidelines regulating the use of media aggregation services. The policy states that information obtained through this surveillance tool may be used for "legitimate law enforcement purposes or other official business of the NYPD," an expansive assertion that offers no real insight into when the NYPD deems it appropriate to use media aggregation services for the systematic collection and automated analysis of vast swaths of New Yorkers' data. Media

[3] *See* New York City Police Department, "Media Aggregation Services: Impact & Use Policy," January 11, 2021, https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-act/media-aggregation-services-nypd-impact-and-use-policy-draft-for-public-comment_01.11.2021.pdf.

aggregation services may be used "in any situation" a supervisor deems appropriate, with few if any stated guidelines for, or constraints upon, supervisory approval.

Third, while the policy notes that the surveillance of political activity is cabined by the Handschu Consent Decree, it fails to describe in what manner or how the NYPD interprets the decree to apply to media aggregation services. In particular, while the Handschu Decree restricts investigations of political activity to the Intelligence Division, it is not clear whether the discovery or targeting of political activity through a media aggregation tool would constitute an investigation covered by the Decree.

Fourth, the NYPD's draft policy does not explain how data from media aggregation services is safeguarded from misuse or unauthorized sharing. With respect to safety, security, retention, access, and use of the data arising from these tools, the policy offers boilerplate assurances that access to these technologies is "critically limited," but does not clarify what that means in practice.

Fifth, the policy states that the NYPD purchases these services from "approved vendors" but does not provide the identity of these vendors. Public records indicate that one vendor with which the NYPD has contracted for similar services is Dataminr,[4] which has been criticized for facilitating the surveillance of Black Lives Matter protesters, raising concerns that the NYPD may be using this tool to monitor protesters in New York City.[5] Without specific information about the vendor, neither the public nor the City Council can conduct an adequate review of the vendor's privacy practices or its fidelity to the spirit of the POST Act. Additionally, 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.

Finally, the draft policy lacks sufficient guarantees for internal audits and oversight mechanisms, as required by the POST Act. The relevant section indicates that the use of these tools must be "discussed with a supervisor," a laughably weak requirement that imposes no constraints whatsoever. Indeed, the audit section does not provide for regular audits, offering instead that an ill-defined list of personnel and units may make "requests for focused audits of computer activity," while providing no insight as to how these tools will be evaluated for accuracy, false positives, misuse, or other factors. The NYPD must require and implement regular audits of its media aggregation services, assess the effectiveness, accuracy, use, and impact of these tools, and make the results available to the public.

[4] Millions March NYC v. New York City Police Department, No. 100690/2017 (N.Y. 2017) (order granting in part petitioner's request) https://www.documentcloud.org/documents/5684800-Millions-March-Nypd.html#document/p1.

[5] Sam Biddle, "Police Surveilled George Floyd Protests with Help from Twitter-Affiliated Startup Dataminr," The Intercept, July 9, 2020, https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/.

II. Social Network Analysis Tools[6]

Social network analysis tools automate the process of reviewing, processing, and collecting information from users' social media profiles, including audio, video, images, location, and other relevant information. As with the media aggregation services policy, the expressed justification for these tools is extremely broad: "legitimate law enforcement purposes or other official business of the NYPD." This is insufficiently specific to offer the public insight regarding the use of these tools. The draft policy also does not provide information on how these tools operate – for example, if they rely on web scraping – or how the information they collect is analyzed or integrated into the NYPD's other surveillance systems, such as its data analysis tool.

Moreover, according to its draft policy, the NYPD purchases social network analysis tools and associated equipment from third party vendors. However, as with the media aggregation services, the policy lacks an integral piece of information: who produces the tools the NYPD uses.

In addition, the NYPD's draft disclosure states that the information it collects "is limited to publicly available information or information that is viewable as a result of user-selected privacy settings *or practices*" (emphasis added). Because user practices could include unknowingly accepting a "friend" or "follow" request from an undercover officer posing as someone else – an NYPD tactic that is allowed pursuant to its 2012 policy on the use of social networks for investigative purposes[7] – these tools could be used not just to obtain publicly available information but to facilitate covert connections. If social network analysis tools are used to analyze and exploit data collected through covert connections, the policy should be transparent about this use and specify what guardrails (if any) the NYPD has in place to protect privacy and civil rights.

The policy also currently does not specify which NYPD units and subdivisions may have access to social media analysis tools or the information they generate. This is critical information in light of other documented abuses of civil rights and civil liberties by units of the NYPD. In the aftermath of 9/11, for instance, it was the anodyne-sounding "Demographics Unit" that conducted large-scale surveillance on Muslim Americans in mosques, universities, and businesses, despite the dearth of any evidence of a real

[6] *See* New York City Police Department, "Social Network Analysis Tools: Impact & Use Policy," January 11, 2021, 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.

[7] New York City Police Department, "Use of Social Networks For Investigative Purposes — General Procedure," Operations Order No. 34, September 5, 2012, https://cdn.muckrock.com/foia_files/1-13-15_MR14466_RES_ID2014-PL-11102.pdf.

connection to terrorist activities.[8] As with the media aggregation services policy, this policy references the Handschu Decree with respect to political investigations but does not explain under what circumstances it would govern use of these tools.

Similar to the media aggregation services policy, the social network analysis tools policy does not provide sufficient specificity when it comes to security of the data. With regard to safeguards and security measures against unauthorized access, the disclosure simply states that access to the tools is "critically limited" and password protected. The POST Act requires more than a mere recitation that access to the tools is "critically limited" and a brief password requirement to guarantee the civil liberties of all New Yorkers.

Finally, as above, the NYPD must provide for regular, publicly available audits that assess the effectiveness, accuracy, and disparate impact of these tools.

III. Internet Attribution Management Infrastructure[9]

Internet attribution management infrastructures are technological tools that allow police to reduce or eliminate the extent to which their digital footprint can be traced. They can be deployed on computer servers, modems, officer laptops, or even smartphones. The NYPD's draft impact and use policy imposes no limits upon the use of these powerful tools, stating that internet attribution management infrastructure may be used "in any situation" that supervisors deem appropriate. It is unclear whether officers or supervisory personnel are even required to document the use of the technology.

This technology will also facilitate the ability of officers to conduct covert surveillance of juveniles online, which poses special risks. Youth of color have been targets of social media surveillance, with the most high-profile cases arising in the context of gang surveillance.[10] The NYPD used social media to target Jelani Henry, a teenage boy, and arrest him in 2012 for gang activity based in part on Facebook "likes" of posts connected to the gang Goodfellas.[11] While it does not appear that this software was used in that

[8] Bridge Initiative Team, "Factsheet: The NYPD Muslim Surveillance And Mapping Program," Bridge Initiative, May 11, 2020, https://bridge.georgetown.edu/research/factsheet-the-nypd-muslim-surveillance-and-mapping-program/.

[9] *See* New York City Police Department, "Internet Attribution Management Infrastructure: Impact and Use Policy," January 11, 2021, https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-act/internet-attribution-management-infrastructure-nypd-impact-and-use-policy-draft-for-public-comment-01.11.2021.pdf.

[10] Rachel Levinson-Waldman, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges," *Howard Law Journal* 61 (2018): 525.

[11] Ben Popper, "How the NYPD Is Using Social Media to Put Harlem Teens behind Bars," The Verge, December 10, 2014, https://www.theverge.com/2014/12/10/7341077/nypd-harlem-crews-social-media-rikers-prison.

particular case, because internet attribution management infrastructure obscures the identity of a police officer, minors may not be aware they are being contacted by an officer.

Finally, mere supervisory discussion is an insufficient oversight measure. As with social media analysis tools, this section must provide for regular, publicly available audits that assess the effectiveness, accuracy, and disparate impact of internet attribution management infrastructure.

***

The NYPD has failed to meet its obligations under the POST Act. It has not adequately disclosed the capacity, use, and impact of its surveillance technologies. The draft impact and use policies described above are clearly deficient and require significant revisions to provide the transparency and oversight required by the POST Act.

Sincerely,

Rachel Levinson-Waldman
Deputy Director

Laura Hecht-Felella
George A. Katz Fellow

Liberty & National Security Program
Brennan Center for Justice at NYU School of Law
120 Broadway, Suite 1750
New York, NY 10271