New York City Council
Committee on Public Safety

Creating Comprehensive Reporting and Oversight of NYPD Surveillance Technologies
December 18, 2019

Written testimony of
Genevieve Fried, Technology Fellow, AI Now Institute

Good afternoon Chairman Richards and members of the Committee on Public Safety. My name is Genevieve Fried and I am a Technology Fellow at the AI Now Institute, an interdisciplinary research institute at New York University that focuses on the social implications of artificial intelligence. The AI Now Institute respectfully submits the following testimony on Int. 0487, the Public Oversight of Surveillance Technology Act (POST Act).

During the 2017 Public Safety Committee hearing on this bill, the NYPD suggested that compliance with the POST Act requirements could allow adversaries to game and subvert NYPD's surveillance technology, putting New Yorkers' public safety at risk.[1] As a Computer Scientist by training with a background in the development and deployment of the machine learning and data-driven systems that drive surveillance technology, I submit the following testimony today with two goals: (1) to assure the Committee that the NYPD's claims are unfounded because the public disclosure requirements in the POST Act do not present a risk to public safety, and (2) that the POST Act is a necessary policy intervention because it provides a meaningful increase in transparency that will promote democratic oversight and will build trust between the NYPD and the communities it serves.

The POST Act Public Disclosure Requirements Do Not Present a Risk to Public Safety

Concerns that the POST Act poses a risk to public safety are unwarranted. The POST Act requires a relatively modest level of public disclosure, namely: "a description and capabilities of a surveillance technology," "rules, processes and guidelines issued by the department regulating access to or use of such surveillance technology," and "policies and/or practices relating to the retention, access, and use of data." This information provides valuable insight to the public, but is not sufficiently detailed for someone to game the system and threaten public safety.

To game a surveillance system, one would need to know far more granular details about it. At a minimum, one would need to know the specific data and datasets it uses as inputs, the systems or algorithms used to parse that data, the outputs presented by those algorithms, the strategies by which the surveillance systems are deployed, and how those strategies are implemented in practice. This type of

[1] Prendergast, D. (2017, June 18). NYPD Anti-terror Chief: Surveillance Bill Would Help Terrorists. *New York Post.* Retrieved from https://nypost.com/2017/06/18/nypd-anti-terror-chief-surveillance-bill-would-help-terrorists/; Winston, A. (2017, July 7). NYPD Attempts to Block Surveillance Transparency Law with Misinformation. *The Intercept.* Retrieved from https://theintercept.com/2017/07/07/nypd-surveillance-post-act-lies-misinformation-transparency/.

disclosure would almost certainly include schematics, design documents, and often direct access to source code and the algorithms at issue. Moreover, given that many policing technologies are not actually applied in ways that are expected or desired,[2] even knowing the strategies behind surveillance technology does not necessarily allow for gaming of that technology as operationalized by a specific agency. One would also need to know how the surveillance tool interacts with other tools that are being used and how the NYPD uses surveillance tools in connection with specific investigations or types of investigations. The POST Act does not require any of this information to be disclosed.

Far from revealing the precise manner in which someone might evade or defeat the surveillance tool, the POST Act only admits that a system is in use, which bodies have access to this system, and whether there are policies or practices in place to regulate the retention, access, and use of data. We know that this type of public disclosure does not impede the efficacy of a given surveillance tool. For example, wiretaps remain a powerful investigative tool despite widespread public knowledge of their existence and the rules governing their use.[3]

In addition, since the NYPD's statement on risk to public safety in 2017, numerous other municipalities across the country have adopted ordinances mandating the publication of far more information on surveillance technology as well as civilian oversight of police surveillance. Seattle[4] and California's Oakland,[5] Berkeley,[6] and Davis[7] have all barred municipal police from deploying new surveillance technology without approval from the city council. San Francisco adopted these measures while also banning the use of facial recognition by police altogether.[8] Though public safety concerns were raised during the deliberations of these ordinances, each measure passed unanimously or near-unanimously and now provide the public with far more information than the POST Act requires.

---

[2] Green, B., & Chen, Y. (2019). Disparate Interactions: An Algorithm-in-the-Loop Analysis of Fairness in Risk Assessments. Proceedings of the ACM Conference on Fairness, Accountability, and Transparency (FAT*). Retrieved from https://www.benzevgreen.com/wp-content/uploads/2019/02/19-fat.pdf; Bond-Graham, D., & Winston, A. (2013, October 30). All Tomorrow's Crimes: The Future of Policing Looks a Lot Like Good Branding. *SF Weekly News*. Retrieved from https://archives.sfweekly.com/sanfrancisco/all-tomorrows-crimes-the-future-of-policing-looks-a-lot-like-good-branding/Content?oid=2827968; Puente, M. (2019, March 12). LAPD data programs need better oversight to protect public, inspector general concludes. *Los Angeles Times*. Retrieved from https://www.latimes.com/local/lanow/la-me-ln-lapd-data-20190312-story.html

[3] Wiretap Reports. (n.d.). *United States Courts*. Retrieved from https://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports

[4] The Surveillance Ordinance. (n.d.). *Seattle Information Technology*. Retrieved from https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies/about-surveillance-

[5] PAC Surveillance Technology Ordinance Approved by City Council. (2018, September 13). *City of Oakland.* Retrieved from https://www.oaklandca.gov/resources/pac-surveillance-technoloy-ordinance-approved-by-city-council

[6] BondGraham, D., (2018, March 14). Berkeley Council Approves Surveillance Technology Oversight Ordinance. *East Bay Express*. Retrieved from https://www.eastbayexpress.com/SevenDays/archives/2018/03/14/berkeley-council-approves-surveillance-technology-oversight-ordinance

[7] Milne, S. (2018, March 21). Davis to Regulate Hi-Tech Surveillance. *Capital Public Radio*. Retrieved from http://www.capradio.org/articles/2018/03/21/davis-to-regulate-hi-tech-surveillance/

[8] Dastin, J. (2019, May 14). San Francisco votes to ban city use of facial recognition technology. *Reuters*. Retrieved from https://www.reuters.com/article/us-san-francisco-facial-recognition/san-francisco-votes-to-ban-city-use-of-facial-recognition-technology-idUSKCN1SK2NH

Litigation and advocacy in other jurisdictions has also required local law enforcement to publicly release more detailed information about surveillance technologies than required by the POST Act. For example, earlier this month the City of New Orleans was ordered to comply with a public records request regarding the locations of the City's surveillance cameras.[9]

To date, there has been no evidence that the public disclosure required by municipal ordinances or litigation has resulted in any public safety threats.

The POST ACT Promotes Democratic Oversight and Public Trust

The stakes of municipal surveillance technology are incredibly high.[10] An important aspect of this technology is its wide scope: many people, even those who are not and never will be under investigation, can be tracked and affected by these systems. There is no functional way to opt-out. For instance, New Yorkers who do not want to be tracked by one of the at least 20,000 cameras around New York City that connect to the NYPD's Domain Awareness System[11] would have to avoid going into the city. In some cases, this inability to opt-out poses additional risks to an individual or community's safety and sense of belonging. For instance, the surveillance technology commonly known as Stingrays mimic cell site towers to allow the NYPD to identify a person's cell phone location. This interferes with the ability for all cellphones in the vicinity to connect with actual cell site towers, which means that when a Stingray is deployed, individuals in its range will not be able to make or receive calls, including calls to emergency services. Even if such disruption is temporary, it can have serious consequences.

Communities of color and low-income New Yorkers are the most vulnerable to this type of pervasive surveillance. A history of racialized policing practices in New York City raises concerns that surveillance technology will disproportionately burden the urban poor and minorities. NYPD's in-house predictive policing system raises this concern.[12] The algorithms underlying predictive policing systems learn patterns based on historical crime data. Yet as researchers and advocates have demonstrated, this data reflects not the prevalence of crime but rather policing practices and policies.[13] This is particularly true in New York,

---

[9] In Win For Civil Rights Groups and Public Defenders, Appeals Court Orders New Orleans to Turn Over Surveillance Camera Locations. (2019, December 6). *Southern Law Poverty Center*. Retrieved from https://www.splcenter.org/presscenter/win-civil-rights-groups-and-public-defenders-appeals-court-orders-new-orleans-turn-over

[10] Green, B. (2019, June 27). Smile, Your City Is Watching You. *New York Times*. Retrieved from https://www.nytimes.com/2019/06/27/opinion/cities-privacy-surveillance.html

[11] A Conversation with Jessica Tisch '08. (2019, July 17). *Harvard Law Today*. Retrieved from https://today.law.harvard.edu/a-conversation-with-jessica-tisch-08/

[12] 'Red Flags' as New Documents Point to Blind Spots of NYPD 'Predictive Policing'. (2019, July 15). *Daily Beast*. Retrieved from https://www.thedailybeast.com/red-flags-as-new-documents-point-to-blind-spots-of-nypd-predictive-policing

[13] Lum, K., & Isaac, W. (2016). To Predict and serve? *Significance*, 13(05). doi: 10.1111/j.1740-9713.2016.00960.x
Richardson, R., Schultz, J. M., & Crawford, K. Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. New York University Law Review Online. Retrieved from https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/

where millions of stop-and-frisk encounters–a practice ruled unconstitutional in 2013–constitute the data of crime-forecasting systems.[14]

Given the stakes of police surveillance technology, there is significant value in the public having knowledge about what systems may be affecting their lives and whether the NYPD has rights-preserving safeguards in place. Yet there currently exists a dearth of information—let alone ways of accessing information—about what surveillance technology the NYPD uses. Most of what we currently know about the surveillance technologies NYPD employs is based on documentation released following costly FOIL litigation, investigative journalism, and inquiries by the criminal defense community and researchers. These efforts have shown that surveillance technologies are pervasive in New York City and that they have unfettered reach, tracking and implicating even those who are not, and may never be, under investigation.

For example, public records request revealed that the NYPD gang database under the de Blasio is massively expanding under vague and sweeping criteria that dictate inclusion in the database. Marne Lenox, an attorney at the NAACP Legal Defense and Educational Fund, described this system as "criminalizing friendships."[15] Individuals do not receive notification when they are added to the database and there are no clear processes to challenge one's inclusion in it. The NYPD has not clarified fundamental questions such as how the database is maintained and purged, nor who has access to it. Several organizations have filed public records requests to find out more, which the NYPD has largely evaded.

These grievances are at the heart of the motivation for the POST Act. NYPD's continual resistance to engage with transparency, denying freedom of information act requests, discovery requests, and legislation, is highly damaging. Lack of transparency impedes civil rights and liberties, but it also undermines public trust. The NYPD's opacity contributes to a climate of suspicion about what surveillance technology is actually in place and how it is used. When the public eventually learns information about the NYPD's practices or tactics, it often confirms their worst fears. A notable example are the recent revelations about the NYPD's quota system that rewarded officers for arresting Black and Latinx residents.[16] The NYPD has argued that the public should trust them to use surveillance technologies safely and lawfully,[17] but the relationship between communities and the NYPD is not strong

---

[14] Richardson, R., Schultz, J. M., & Crawford, K. Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. New York University Law Review Online. Retrieved from https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/

[15] Speri, A. (2018, June 11). New York Gang Database Expanded by 70 Percent Under Mayor Bill De Blasio. *The Intercept*. Retrieved from https://theintercept.com/2018/06/11/new-york-gang-database-expanded-by-70-percent-under-mayor-bill-de-blasio/

[16] Brown, S. R., & Rayman, G. (2019, December 5). Ex-cop details NYPD 'collar quotas' -- arrest black and Hispanic men, 'no cuffs on soft targets' of Jews, Asians, whites: court docs. *Daily News*. Retrieved from https://www.nydailynews.com/new-york/nyc-crime/ny-nypd-quotas-lawsuit-20191205-osdwj4kounf5xkvurkj3wshqry-story.html

[17] McCormack, S. (2015, October 2). NYPD Says 'Trust Us' on Potentially Dangerous X-Ray Vans Roaming the Streets of New York. ACLU. Retrieved from https://www.aclu.org/blog/privacy-technology/surveillance-technologies/nypd-says-trust-us-potentially-dangerous-x-ray

enough for this approach to be viable. It is advantageous for police-community relations for the NYPD to be more forthcoming about the surveillance technologies it uses, how that use is regulated, and how data is retained, accessed, and applied. The impact assessments mandated by the POST Act offer the opportunity to promote transparency in a way that could significantly build trust across stakeholders and could provide democratic oversight to the public—whose tax dollars pay for these systems and on whose behalf these systems are deployed.

A loss of privacy and a lack of democratic input are not the inevitable outcomes of new technology. It is up to bodies such as the New York City Council to ensure that technological innovation is grounded within public transparency and accountability. The POST Act provides a necessary measure of public disclosure to NYC residents about how they are being surveilled without posing a public security risk. This type of transparency is necessary for a robust discourse about the social utility of surveillance technology.

Thank you for your time.