epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

NEW YORK CITY POLICE DEPARTMENT

POST Act Disclosures

February 25, 2021

In compliance with the Public Oversight of Surveillance Technology (POST) Act, the New York City Police Department ("NYPD") published on January 11th, 2021 36 draft policies regarding information about surveillance technologies the NYPD.[1]

EPIC submits these comments to (1) urge the NYPD to address the invasive mass surveillance these technologies create through more robust policy disclosure and decommissioning certain technology, and (2) draw attention to concerns about specific technologies used by the NYPD. EPIC submits these comments in addition to comments submitted by a coalition of 14 organizations and leading researchers concerning insufficient disclosures and process issues regarding NYPD's compliance with the POST act.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has litigated cases against the Department of Justice to compel production of documents regarding "evidence-based risk assessment tools"[2] and the Department of Homeland Security to compel production of documents

[1] New York Police Department, *POST Act; Draft policies for Public Comment* (January 11, 2021), https://www1.nyc.gov/site/nypd/about/about-nypd/public-comment.page.

[2] EPIC, *EPIC v. DOJ (Criminal Justice Algorithms),* https://epic.org/foia/doj/criminal-justice-algorithms/.

about a program to "assess" the probability that an individual commits a crime.[3] EPIC has led a campaign calling for a moratorium on face surveillance,[4] highlighted the disproportionate risk of traffic stops based on inaccurate data in a U.S. Supreme Court amicus brief,[5] published a report about Pretrial Risk Assessment Tools[6], and advocates for algorithmic transparency and accountability.

Several policies published by the NYPD pose an impermissible risk of exacerbating racial disparities throughout the criminal justice system and continuing a sweeping mass surveillance state. In this comment, EPIC will point to specific concerns about Facial Recognition[7]; License Plate Readers[8] ("LPR"); Manned[9] and Unmanned[10] Aircraft Systems; and Social Network Analysis Tools[11].

I. NYPD's POST Act Disclosures Show New Yorkers are Subject to Constant Invasive Dangerous Mass Surveillance

Taken together, the 36 policies that the NYPD disclosed as part of the POST act paint a picture of layered surveillance and exacerbated risks of police encounters for marginalized

[3] *See Id.* and EPIC, *EPIC v. DHS (FAST Program),* https://epic.org/foia/dhs/fast/.

[4] EPIC, Ban Face Surveillance, https://epic.org/banfacesurveillance/.

[5] EPIC Amicus Brief, *Kansas v. Glover*, 139 S. Ct. 1445 (2019), https://epic.org/amicus/fourth-amendment/glover/EPIC-Amicus-Kansas-v-Glover.pdf.

[6] EPIC, *Liberty At Risk: Pre-trial Risk Assessment in the Criminal Justice System*,http://epic.org/libertyatrisk.

[7] New York Police Department, *Facial Recognition Impact and Use Policy*, Jan. 11, 2021, 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.

[8] New York Police Department, *License Plate Readers Impact and Use Policy*, Jan. 11, 2021, 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.

[9] New York Police Department, *Manned Aircraft Systems Impact and Use Policy*, Jan. 11, 2021, https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-act/manned-aircraft-systems-nypd-impact-and-use-policy-draft-for-public-comment-01.11.2021.pdf.

[10] New York Police Department, *Unmanned Aircraft Systems Impact and Use Policy*, Jan. 11, 2021, 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.

[11] New York Police Department, *Social Network Analysis Tools Impact and Use Policy*, Jan. 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.

communities. Certain technologies such as facial recognition, iris recognition, license plate readers, and more run the risk of inaccurate results, felt disproportionately by black communities.[12] Concurrently, technologies such as vehicle mounted cameras, body worn cameras, covert and overt recording devices, and Wi-Fi Geo location devices increase the degree to which every New Yorker is surveilled regardless of their actions. Further, synthesis systems such as social network analysis tools, data analysis tools, domain awareness system, and more mix the data flows and use this potentially inaccurate data exacerbating potential negative effects of inaccuracy or impropriety at any one single point. The under reporting of key information in a majority of these policies undermine the purpose of the POST Act and places New Yorkers at a disadvantage in trying to fully understand how their Police Department is surveilling them.

Particularly, the vast majority of policies fail to name the vendor that created the technology, what training policies there are for the technology, and what the data retention and minimization policies are. The lack of detailed disclosure runs contrary to the POST Act, which is an act to "creat[e] comprehensive reporting and oversight of New York city police department surveillance technologies."[13] To comply with the law, EPIC urges the NYPD to elaborate on which vendor the NYPD contracted with for every surveillance technology, who is performing training, what constitutes successful use of each technology, and publish regular schedules of independent audits. This would help both the NYPD and the public understand the procurement decisions made by the NYPD, and how the technologies adopted impact New Yorkers.

[12] *See, e.g,, NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, National Institute of Standards and Technology, December 19, 2019, https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software; Meiling Fang et. al, *Demographic Bias in Presentation Attack Detection of Iris Recognition Systems*, Jul. 2020, https://arxiv.org/pdf/2003.03151.pdf.

II. Technologies used by the NYPD have biased effects on underserved communities

The NYPD uses several technologies that have been demonstrated by researchers and borne out in real-life examples to disproportionately target and harm poorer communities, communities of color, women, and other marginalized groups. In this section, EPIC will highlight those issues for Facial Recognition, License Plate Readers, Manned and Unmanned Aircraft Systems, and Social Network Analysis systems, and recommend improvements regarding the NYPD's currently disclosed use of them.

a. Facial Recognition

The NYPD draft policy for their use of Facial Recognition states that "some studies have found variations in accuracy for some software products in analyzing the faces of African Americans, Asian Americans, women, and groups other than non-white males."[14] The dire conclusions of these studies is underemphasized in this disclosure. The referenced study asserting that "hybrid machine/human systems" mitigate some of those negative effects is not cited directly. Furthermore, the NYPD doesn't detail how the hybrid model is adopted in its use of facial recognition and how the model mitigates the specific racialized harms exacerbated by the department's use of the technology.

A landmark study from the National Institute of Standards and Technology ("NIST") in 2019 analyzed the facial recognition algorithms of a "majority of the industry" and found the software up to 100 times more likely to return a false positive of a non-white individual than white individuals.[15] Specifically, NIST found "for one-to-many matching, the team saw higher rates of false positives for

[14] New York Police Department, *Facial Recognition Impact and Use Policy*, Jan. 11, 2021, 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.

[15] *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, National Institute of Standards and Technology, December 19, 2019, https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

African American females," which they highlight "are particularly important because the consequences could include false accusations."[16] Another study demonstrated an error rate disparity of 33.9% for dark-skinned women when compared to light-skinned men.[17] There are no shortage of specific examples of facial recognition software misidentifying black people, and black women specifically, at a significantly high rate. The failure of the NYPD to disclose which software it uses and independent validation studies, among other important information needed to evaluate the use of the technology, endangers New Yorkers, especially when facial recognition is used to locate black protestors of racial violence.[18]

Beyond the insufficient consideration of research on facial recognition, the NYPD use and impact policies incorrectly state their facial recognition software "does not use artificial intelligence, machine learning, or any additional biometric measuring technologies." EPIC urges the NYPD to suspend the use of facial recognition technology. During the suspension, the NYPD should disclose more information regarding the developer, the software, and specific efforts to mitigate the disproportionate impact on black communities—complete with publicly available benchmarks the department must meet to keep using the technology.

b. License Plate Readers

License plate readers (LPRs) or automated license plate readers (ALPRs) enable comprehensive location tracking, are prone to consequential errors, and are often disproportionately deployed against Black communities. License plate readers capture images of license plates and translate those images to searchable text. This technology allows the NYPD to create a database of

[16] *Id.*

[17] Larry Hardesty, *Study finds gender and skin-type bias in commercial artificial-intelligence systems*, MIT News (February 11, 2018), https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

[18] *See, e.g* George Joseph, Jacke Offenhartz, *NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist's Apartment*, Gothamist (Aug. 14, 2020), https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment.

recorded hits, mapping where and when license plates are scanned. LPRs are mass surveillance tools in two ways. First, they permit both historical and real-time location tracking of individuals movements through the network of car-mounted and stationary LPR cameras. Second, LPRs are not precise instruments. They sweep up the license plates of every passing car, pulling data from thousands of citizens into NYPD's database each day. In 2016, the NYPD was capturing more than 1 million LPR images per day and adding that data to the Domain Awareness System (DAS).[19] Because license plate readers are passive systems, they collect information for the NYPD without any form of individualized suspicion. Such systems require strict controls on access to the resulting data and short data-retention times to mitigate the risk of comprehensive public surveillance.

License plate readers are prone to errors that expose citizens to harmful and unnecessary traffic stops. The New York Court of Appeals recently found that a positive LPR identification alone is insufficient grounds for a traffic stop.[20] The case arose from a 2014 stop of a vehicle that was incorrectly listed as impounded in a Buffalo, NY police database.[21] The same year, a LPR misread the "7" for a "2" on Kansas City man's license plate, leading local police to pull the man over and approach his car with guns drawn.[22] Similarly in 2019, Bay Area privacy advocate Brian Hofer and his brother were handcuffed and detained by Contra Costa County sheriffs while driving a rental car that had been reported stolen, and recovered, 8 months before.[23] The incident led to a

[19] Rocco Parascondola, *Exclusive: NYPD will be able to track fugitives who drive past license plate readers across the U.S.*, N.Y. Daily News (Mar. 02, 2015), https://www.nydailynews.com/new-york/nypd-track-fugitives-drive-license-plate-readers-article-1.2133879.

[20] *People v. Hinshaw*, 2020 NY Slip OP 04816 (decided Sept. 1, 2020), https://law.justia.com/cases/new-york/court-of-appeals/2020/46.html.

[21] *Id*.

[22] Cyrus Farivar, *Due to license plate reader error, cop approaches innocent man, weapon in hand*, Ars Technica (Apr. 23, 2014), https://arstechnica.com/tech-policy/2014/04/due-to-license-plate-reader-error-cop-approaches-innocent-man-weapon-in-hand/.

[23] Lisa Fernandez, *Sheriff pays East Bay privacy advocate nearly $50K in license plate reader case*, KTVU (Nov. 16, 2020), https://www.ktvu.com/news/sheriff-pays-east-bay-privacy-advocate-nearly-50k-in-license-plate-reader-case.

nearly $50k settlement for Hofer.[24] LPR systems are at most 90 percent accurate.[25] According to Mike Sena, executive director of the Northern California Regional Intelligence Center, an LPR alert is, "just the pointer to say, 'look at the license plate in a little more detail.' Call it into a dispatcher and make sure it is actually wanted or connected with a subject of an investigation."[26] Any LPR policy must address the risk of false positives to protect citizens from unnecessary and potentially dangerous traffic stops.

License plate readers also disproportionally surveil low-income and minority communities. For example, an analysis of eight days of ALPR data from Oakland, California—covering over 63,000 license plate scans and over 48,000 unique plates—revealed that lower income neighborhoods, as well as those with high black and Latino populations, were disproportionately captured by ALPR patrols.[27] In Oakland, LPR use corresponded closely with poverty and minority populations, but not with high-crime areas.[28] Although there is no direct data on LPR distribution in New York City, NYPD officers are a more frequent presence in poor and gentrifying neighborhoods.[29] As the NYPD mounts LPRs on squad-cars, it stands to reason that poor and minority neighborhoods are subjected to more LPR scans. Police departments must actively address

[24] *Id.*
[25] Lisa Fernandez & Brooks Jarosz, *Privacy advocate sues CoCo sheriff's deputies after license plate readers target his car stolen*, KTVU (Feb. 15, 2019), https://www.ktvu.com/news/privacy-advocate-sues-coco-sheriffs-deputies-after-license-plate-readers-target-his-car-stolen.
[26] *Id.*
[27] Dave Mass and Jeremy Gillula, *What You Can Learn from Oakland's Raw ALPR Data*, EFF (Jan. 21, 2015), https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data.
[28] *Id.*
[29] *See e.g.*, Luke Scrivener et al., *Tracking Enforcement Trends in New York City: 2003-2018*, Data Collaborative for Justice (Sept. 2020), https://datacollaborativeforjustice.org/wp-content/uploads/2020/09/2020_08_31_Enforcement.pdf (finding that Black neighborhoods are patrolled and policed at a higher rate than white neighborhoods); Harold Stopper, *New Neighbors and the Over-Policing of Communities of Color*, Community Service Society NY (Jan. 6, 2019), https://www.cssny.org/news/entry/New-Neighbors (finding substantially higher rates of 311 and "quality of life" 911 calls draw police presence into gentrifying neighborhoods with majority-minority populations).

the overuse of surveillance technologies on minority communities. That process starts with recognizing the potential disparate impact, and then taking steps to reduce it.

NYPD's license plate reader policy does nothing to address these concerns.[30] The document fails to put in place meaningful limits on police use of LPR search functions, permitting open-ended searches of the Department's LPR database. Furthermore, the document does not require officers to confirm the identity of a car flagged by a LPR, magnifying the likelihood of a harmful false-positive traffic stop. And the Department has not reckoned with heavier deployment of LPRs in minority neighborhoods, much less taken steps to address this discrepancy. The draft policy uses only boilerplate language in its disparate impacts section, instead of providing a real analysis of LPRs. In its present state, the Draft LPR Policy displays a deliberate indifference to the privacy harms caused by license plate readers.

EPIC urges the NYPD to implement meaningful limits on LPR searches, including requiring a warrant for long-term queries. The Department can protect citizens and conserve resources by requiring officers to confirm vehicle identity before initiating a stop based on an LPR alert. EPIC also urges the NYPD to reduce its LPR database retention time to at most three months, safeguarding citizens from long-term location tracking. Finally, the NYPD should use the POST Act policy as a vehicle to address potential disparate impacts of LPR use.

c. Manned and Unmanned Aircraft Systems

Aerial surveillance is performed by both manned and drone aircrafts. Technologies including cameras, cell-site simulators, and thermal imaging devices pose a particularly unique threat to the public when attached to aircraft due to the overwhelming amount of information that can be

[30] New York Police Department, *License Plate Readers Impact and Use Policy*, Jan. 11, 2021, 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.

collected from an aerial vantage point. Manned and unmanned aircraft implement mass surveillance by allowing the NYPD the unprecedented ability to record individuals' public movements on a grand scale.

Heavy use of surveillance aircraft can create detailed records of public movements over a long period. A single Cessna aircraft deployed in Baltimore can record over 30 square miles of terrain in high definition.[31] This type of monitoring creates a permanent record of individuals movements, and that of their vehicles. As a further example, between May 29th and June 16th, 2020, NYPD helicopters logged more than 180 hours covering Black Lives Matter protests.[32] Long-term use of surveillance aircraft poses a particular threat of comprehensive location tracking. Use of aircraft at protests allows detailed monitoring of First-Amendment protected activity. As former police officer and professor Brian Higgins explains, aircraft "can identify people, literally pick out who's doing what. Who's carrying objects. Who's organizing."[33]

The same aircraft often intimidate protesters, chilling free expression. Helicopters in NYC this summer flew as low as 100ft over protesters.[34] City Councilman and protester Brad Lander described his reaction to those low flights, "It was really intimidating. To me, it feels pretty clear that that was really the point…"[35] The U.S. military routinely uses low-flying helicopters as a crowd-

[31] Monte Reel, *Secret Cameras Record Baltimore's Every Move From Above*, Bloomberg (Aug. 23, 2016), https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/.
[32] Stephen Nessen, How Low Did Those NYPD Helicopters Go At Recent Protests?, Gothamist (Jun. 23, 2020), https://gothamist.com/news/how-low-did-those-nypd-helicopters-go-recent-protests.
[33] *Id.*
[34] *Id.*
[35] *Id.*

control and intimidation technique abroad.[36] Hand-launched drones provide police with similar intelligence-gathering capabilities, and their close proximity to protesters can be seen as a threat.[37]

NYPD's draft policies for manned and drone aircrafts fail to engage with the extensive privacy threats from aerial surveillance in a meaningful way. Under the current rules, operating drone aircraft over protests is a per se permissible use.[38] NYPD's manned aircraft policy has no defined permissible uses whatsoever, and submits only "private assistance" to high-level scrutiny.[39] EPIC urges the NYPD to impose stricter limits on surveillance aircraft use that recognize the massive amounts of information aircraft collect from a broad segment of the public. Use of surveillance aircraft should be strictly limited to well-defined emergency situations and carefully audited to retain only limited data.

d. Social Network Analysis Tools

Social network analysis (SNA) tools can automatically monitor social network accounts, perform powerful searches across social media, and store social media posts. These tools enable sweeping surveillance through keyword searches across social media, identification of "otherwise unknown connections" between individuals, and automated tracking.[40] SNA tools are regularly deployed against protesters, monitoring First Amendment protected content.[41] When used in

[36] Alex Horton et al., *A low-flying 'show of force'*, Washington Post (Jun. 23, 2020), https://www.washingtonpost.com/graphics/2020/investigations/helicopter-protests-washington-dc-national-guard/ ("the use of a helicopter's rotor wash is a common military tactic to incite fear, disperse crowds and warn of other capabilities, like rockets and guns, said Kyleanne Hunter, a former Marine Corps pilot who flew Cobra attack helicopters in Iraq and Afghanistan.").

[37] Faine Greenwood, *Can a Police Drone Recognize Your Face?*, Slate (Jul. 8, 2020), https://slate.com/technology/2020/07/police-drone-facial-recognition.html.

[38] New York Police Department, *Manned Aircraft Systems Impact and Use Policy*, Jan. 11, 2021, https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-act/manned-aircraft-systems-nypd-impact-and-use-policy-draft-for-public-comment-01.11.2021.pdf.

[39] New York Police Department, *Unmanned Aircraft Systems Impact and Use Policy*, Jan. 11, 2021, 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.

[40] New York Police Department, *Social Network Analysis Tools Impact and Use Policy*, Jan. 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.

[41] Jeramie D. Scott, *Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space*, 12 J. Bus. & Tech. L. 151 (2017), http://digitalcommons.law.umaryland.edu/jbtl/vol12/iss2/2.

combination with facial recognition, SNA tools become immensely powerful, allowing mass identification of individuals.

The NYPD has a history of surveilling protesters, including Black Lives Matter activists. Emails obtained in the wake of 2014-2015 Black Lives Matter protests in New York revealed "extensive surveillance" of protesters and activists.[42] This surveillance continued in 2020, when among many instances of social media surveillance, an image from Instagram was apparently used to identify activist Derrick Ingram.[43] That identification led to a well-documented siege of Ingram's apartment.[44] These are not isolated instances, but examples of a trend of disparate impact in digital surveillance. Scholars have warned for years that social media analysis has the potential to magnify issues of bias through "everyday racism in digital policing".[45] NYPD must be careful to avoid surveilling First Amendment protected activity, and to address the potential for radically different surveillance of minority groups.

The NYPD's draft SNA policies fall short of the measures required to constrain police deployment of social network analysis tools to appropriate and Constitutional uses. The draft policy places few limits on how officers use SNA tools, fails to impose stringent auditing requirements, and does not acknowledge that SNA can impinge on First Amendment activity. The policy also disregards the interaction between SNA tools and other surveillance technologies, including facial recognition. EPIC urges the NYPD to limit the use of SNA tools to already-identified suspects, ban

[42] Mark Morales and Laura Ly, *Released NYPD emails show extensive surveillance of Black Lives Matter protesters*, CNN (Jan. 18, 2019), https://www.cnn.com/2019/01/18/us/nypd-black-lives-matter-surveillance.

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

[44] *Id*.

[45] *See e.g.* Desmond Upton Patton et al., *Stop and Frisk Online: Theorizing Everyday Racism in Digital Policing in the Use of Social Media for Identification of Criminal Conduct and Associations*, Social Media + Society (July 2017), https://journals.sagepub.com/doi/10.1177/2056305117733344#articleCitationDownloadContainer.

the use of SNA tools for protest or protest-related monitoring, impose strong auditing requirements, and analyze in the POST Act policy both the interaction of SNA tools with other surveillance tech and the potential disparate impacts of digital surveillance.

Conclusion

The NYPD's POST Act disclosures show that the Department uses technologies that have been proven to be inaccurate, prone to error when used on people of color, and are deployed inequitably. Furthermore, the disclosures are incomplete, and many important sections on powerful technologies remain opaque. EPIC urges the NYPD to consider the dangerous risks of the use of these surveillance tools both individually and as a connected system, and to introduce more safeguards and detail in their final policies.

/s/ *Jeramie D. Scott*
Jeramie D. Scott
EPIC Senior Counsel

/s/ *Jake Wiener*
Jake Wiener
EPIC Law Fellow

/s/ *Ben Winters*
Ben Winters
EPIC Equal Justice Works Fellow