ABOVE THE LAW?

NYPD Violations of the Public Oversight of Surveillance Technology (POST) Act

ELENI MANIS, PHD AND ALBERT FOX CAHN, ESQ.

OCTOBER 7, 2021

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT

This work is made possible by the generous support of our partners at the Calyx Institute.

I. Introduction

This report documents the New York City Police Department (NYPD)'s failure to comply with New York City's Public Oversight of Surveillance Technology Act (POST Act). Enacted in 2020, the POST Act is the first law to oversee the NYPD's use of surveillance technology. A first attempt to regulate NYPD's surveillance tools, the law does not ask much: NYPD is only required to reveal its surveillance tools. Still, the NYPD has twice failed to clear even the low bar set by the POST Act. It failed to make a good faith effort to comply with the POST Act's reporting requirements when it published draft "impact and use" policies for public comment in January 2021. NYPD then failed to respond to the public's requests for more information when it published its revised policies in April 2021. As this report establishes, NYPD falls far short of the reporting norms set by other police departments subject to surveillance technology oversight laws.

II. Concerns Leading to the Creation of the POST Act

In the years preceding the passage of the POST Act, the NYPD actively concealed its use of a host of advanced surveillance technologies. Nearly unconstrained by federal or local oversight, NYPD targeted ordinary New Yorkers with an arsenal of surveillance tools—Stingrays, the Domain Awareness System, X-ray vans, facial recognition, the Gang Database—while denying the public even basic information about its tools and practices.

The NYPD concealed its use of Stingrays, which mimic cellphone towers, to track New Yorkers' locations using their cellphones and to identify targeted individuals and nearby bystanders.[1] From 2008 to May 2015, the NYPD used Stingrays over 1,000 times without a written policy in place and without warrants.[2] StingRay use is rampant and virtually unregulated.[3]

The NYPD secretively operated its Domain Awareness System (DAS), a network of cameras, license plate readers, and radiological sensors that collect data ranging from MetroCard swipes to video footage.[4] By aggregating this data, the NYPD creates a "real-time surveillance map" of New York City capable of tracking individuals as they move about the city and visit sensitive locations such as abortion clinics, political rallies, and mosques.[5] In 2016, the NYPD extended the reach of DAS by

[1] *Stingray Tracking Devices: Who's Got Them?*, ACLU (Nov. 2018), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them ("When used to track a suspect's cell phone, [Stingrays] also gather information about the phones of countless bystanders who happen to be nearby.")..

[2] *NYPD Has Used Stingrays More Than 1,000 Times since 2008*, NYCLU (Feb. 11, 2016), https://www.nyclu.org/en/press-releases/nypd-has-used-stingrays-more-1000-times-2008.

[3] Stephanie K. Pell & Christopher Soghioan, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J. L. & TECH 134, 166 (2013) ("The StingRay, therefore, illustrates a larger gap in congressional oversight insofar as new, invasive surveillance technologies and collection methods not directly authorized by Congress can be used, often for decades, without any reliable notice to Congress about their use.").

[4] Ayyan Zubair, *Domain Awareness System*, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT (Sept. 26, 2019), https://www.stopspying.org/latest-news/2019/9/26/domain-awareness-system; Faiza Patel & Michael Price, *Keeping Eyes on NYPD Surveillance*, BRENNAN CTR. FOR JUST. (June 13, 2017), https://www.brennancenter.org/our-work/analysis-opinion/keeping-eyes-nypd-surveillance.

[5] Ayyan Zubair, *supra* note 4.

purchasing a database of over 2.2 billion license plate reads gathered nationwide.[6] But DAS remained a mystery to the New Yorkers that it tracked.[7]

The NYPD even attempted to refuse to acknowledge its conspicuous X-ray vans.[8] These white vans use "Z-backscatter" X-ray technology to render photo-like depictions of any organic matter—like people—concealed behind cars, walls, or objects.[9] NYPD refused to reveal how many X-ray vans it had, any health effects of the X-ray vans on passersby, or where, when, and how often the vans were used.[10] In 2015, then NYPD police commissioner Bill Bratton attempted to dodge questions about the vans by citing security concerns, saying "I will not talk about anything at all about this. . . ."[11] The courts disagreed, ordering the NYPD to report publicly on its use of X-ray technology.[12]

The NYPD also hid its misuse of facial recognition technology from the public. Police departments typically use facial recognition to try to identify individuals by matching an image of an unknown person to a database of known individuals.[13] Out of public view, the NYPD manipulated images, adding features from other photos and doctoring images to improve the odds of a supposed match—any match.[14] Disconcertingly, prior to the passage of the POST Act, NYPD had no policies restricting the altering of photos.[15]

The NYPD also operated a Criminal Group Database (the "Gang Database") without revealing the criteria used to identify individuals as possible gang members. The Gang database almost exclusively targets BIPOC individuals: 99% of New Yorkers added to the database during its dramatic expansion from 2014 to 2018 were "not white."[16] New Yorkers, including children, are frequently added to the database without every being accused of a crime, let alone given their day in court. But prior to the POST Act, it was not clear what did count: the NYPD did not disclose "the criteria it

[6] Ángel Díaz, *New York City Police Department Surveillance Technology*, Brennan Ctr. for Just. (Oct. 7, 2019), https://www.brennancenter.org/sites/default/files/2019-10/2019_10_LNS_%28NYPD%29Surveillance_Final.pdf.

[7] *Id.*

[8] *See, e.g.*, Conor Friedersdorf, *The NYPD Is Using Mobile X-Ray Vans to Spy on Unknown Targets*, Atlantic (Oct. 19, 2015); Michael Grabell, *Judge Orders NYPD to Release Records on X-ray Vans,* ProPublica (Jan, 9, 2015), https://www.propublica.org/article/judge-orders-nypd-to-release-records-on-x-ray-vans; Simon McCormack, *NYPD Says 'Trust Us' on Potentially Dangerous X-Ray Vans Roaming the Streets of New York*, ACLU (Oct. 21, 2015), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/nypd-says-trust-us-potentially-dangerous-x-ray.

[9] Ángel Díaz, *New York City Police Department Surveillance Technology*, Brennan Ctr. For Just. (Oct. 4, 2019), https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology. *See also Z Backscatter*, Rapiscan Systems, https://www.rapiscan-ase.com/resource-center/technology/z-backscatter-x-ray-imaging (last visited Aug. 16 2021); *Z Backscatter Van (ZBV)*, Homeland Security Tech., https://www.homelandsecurity-technology.com/projects/z-backscatter-van-zbv/ (last visited Aug. 16, 2021).

[10] Conor Friedersdorf, *supra* note 8.

[11] Id.; Yoav Gonen & Shawn Cohen, *NYPD Has Super-Secret X-ray Vans*, N.Y. POST (Oct. 13, 2015), https://nypost.com/2015/10/13/nypd-has-secret-x-ray-vans/.

[12] Michael Grabell, *supra* note 10.

[13] *Id.*

[14] Eleni Manis, Albert Fox Cahn, Naz Akyol, & Caroline Magee, *Scan City*, Surveillance Tech. Oversight Project (July 8, 2021), https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/60e5dd3bed032877ec8e3be9/1625677116317/2021.7.7_Scan+City_FINAL.pdf.

[15] Clare Garvie, *supra* note 15.

[16] Alice Speri, New York Gang Database Expanded by 70 Percent under Mayor Bill de Blasio, Intercept (June 11, 2018), https://theintercept.com/2018/06/11/new-york-gang-database-expanded-by-70-percent-under-mayor-bill-de-blasio; *see also* Ashley Southall, *supra* note 22 ("Nearly everyone in [the database] is Black or Latino, and most have not been convicted of a crime, fueling criticism that the database puts young men under criminal suspicion based primarily on their race.").

uses to add individuals to the database or details of how the list is used, shared, purged, or corrected."[17]

Finally, the NYPD secretly surveilled and retained photographs of protestors in violation of New York court-ordered guidelines.[18] In 2016, the department was forced to reveal that undercover officers had filmed activists at protests and that NYPD had retained photographs of protestors taken in 2014 and 2015.[19] NYPD later used these retained photos to investigating specific individuals.[20] This violates New York's Handschu Guidelines,[21] which prohibit the NYPD from retaining information obtained from visits to public places and events unless it relates to potential unlawful activity.[22] In reality, such content was retained for years.

In the years preceding the passage of the POST Act, the NYPD subjected New Yorkers to a host of Orwellian privacy violations without the public's knowledge and without any real oversight to prevent the abuse of surveillance tools. Unsurprisingly, this burden fell disproportionately on overpoliced groups—particularly BIPOC youth, undocumented immigrants, and protestors. The NYPD's investigatory practices have long disproportionately targeted Black and Brown communities.[23] Technology compounded NYPD's racial bias. East New York in Brooklyn—54.5% Black, 30% Latinx, only 8.4% White—became the most surveilled neighborhood in Manhattan, Brooklyn, or the Bronx.[24] NYPD's surveillance data found its way to the U.S Citizenship and Immigration Services (ICE).[25] NYPD used facial recognition to identify and harass protestors,

[17] *Id.*

[18] *See* George Joseph, *Years after Protests, NYPD Retains Photos of Black Lives Matter Activists*, APPEAL (Jan. 17, 2019), https://theappeal.org/years-after-protests-nypd-retains-photos-of-black-lives-matter-activists/.

[19] *Id.*; George Joseph, *NYPD Sent Undercover Officers to Black Lives Matter Protest, Records Reveal*, GUARDIAN (Sept. 26, 2019), https://www.theguardian.com/us-news/2016/sep/29/nypd-black-lives-matter-undercover-protests.

[20] George Joseph, *supra* note 18.

[21] The Handschu Guidelines are a set of restrictions on police behavior in New York City with respect to political activity. The guidelines were part of a negotiated settlement of a class-action lawsuit, *Handschu v. Special Services Division*, 605 F. Supp. 1384, 1384 (S.D.N.Y. 1985), in which the U.S. District Court for the Southern District of New York found police surveillance of political activity violated plaintiffs' constitutional rights.

[22] *Guidelines for Investigations Involving Political Activity*, https://www.aclu.org/sites/default/files/field_document/2003_v_2017.pdf Section IX.A.2 (2017) ("For the purpose of detecting or preventing terrorist activities, the NYPD is authorized to visit any place and attend any event that is open to the public, on the same terms and conditions as members of the public generally. No information obtained from such visits shall be retained unless it relates to potential unlawful or terrorist activity.").

[23] *See An Investigation of NYPD's Compliance with Rules Governing Investigations of Political Activity*, OIG-NYPD (Aug. 2016), https://www1.nyc.gov/assets/doi/reports/pdf/2016/2016-08-23-Oig_intel_report_823_final_for_release.pdf (detailing how 95% of NYPD intelligence investigations targeted Muslim New Yorkers or individuals associated with Muslims); Lauren del Valle, *NYPD Didn't Substantiate Any Complaints of Police Bias over 4 Years. Report Cites Need to Improve*, CNN (June 27, 2019), https://www.cnn.com/2019/06/27/us/nypd-bias-complaints-report/index.html (noting that the NYPD "did not substantiate a single one of the complaints of biased policing it received between October 2014 and January 2019" despite receiving 2,495 complaints); Alice Speri, *supra* note 16 (noting that of the newly added individuals to the gang member database, 66% were Black and 33% were Hispanic, and that more than 90% of those stopped under stop and frisk in New York were Black and Latino).

[24] *Surveillance City: NYPD Can Use More Than 15,000 Cameras to Track People Using Facial Recognition in Manhattan, Bronx, and Brooklyn*, AMNESTY INTERNATIONAL (June 3, 2021), https://www.amnesty.org/en/latest/news/2021/06/scale-new-york-police-facial-recognition-revealed/.

[25] Albert Fox Cahn, Surveillance by Sanctuary Cities Is Helping ICE Track Undocumented Immigrants¸ NBC NEWS (July 19, 2019), https://www.nbcnews.com/think/opinion/surveillance-sanctuary-cities-helping-ice-track-undocumented-immigrants-ncna1027981.

including Black Lives Matter activist Derrick Ingram.[26] These misuses of technology and others conform with the NYPD's practice of disproportionately targeting certain communities even outside the surveillance context.[27]

This widespread, seemingly unmonitored, and—prior to the POST Act—largely undisclosed use of surveillance technology lay in stark juxtaposition with its staggering costs. The NYPD spent approximately $40 million to create the DAS.[28] The NYPD's X-ray vans cost between $729,000 to $825,000 each—times an unknown total number of vans.[29]

Passage of the POST Act

In light of the NYPD's surveillance abuses and the lack of oversight and transparency, the public and lawmakers began to call for technology oversight legislation. The New York City Council aimed to make the NYPD's use of surveillance technology transparent, including by describing any restrictions on the NYPD's use and articulating what safeguards were in place to protect individuals' privacy.[30] Legislators introduced the POST Act in March 2017. It required the NYPD to disclose information about the technology it used and the safeguards in place to protect information collected.[31] Police officials strongly opposed the bill, arguing that any transparency would aid criminals.[32]

Despite the initial strong pushback, lawmakers were able to pass the POST Act after support for police reform increased following the death of George Floyd at the hands of Minneapolis police officers.[33] New York City Mayor DeBlasio signed the bill into law on July 7, 2020, with reporting

[26] James Vincent, *NYPD Used Facial Recognition to Track Down Black Lives Matter Activist*¸ Verge (Aug. 18, 2020), https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram.

[27] *See, e.g. New Data: Police Disproportionately Target Black and Latino Students in NYC Schools*, ACLU (Apr. 30, 2018), https://www.nyclu.org/en/press-releases/new-data-police-disproportionately-target-black-and-latino-students-nyc-schools (finding that New York City school safety data showed that Black and Latino children are disproportionately arrested, handcuffed, and issued summonses in schools by police); Sean Gardiner, *Report Finds Stop-and-Frisk Focused on Black Youth*, Wall St. J. (May 9, 2012), https://www.wsj.com/articles/BL-METROB-15148 (finding that the numbed of stop-and-frisks performed on Black men ages 14 to 24 by the NYPD outnumbered the city's total population of Black men in that age range and that Black and Latino men ages 14 to 24 account for 416.% of total police stops despite the fact that the demographic makes up 4.7% of the city's population); John Bolger & Alice Speri, *NYPD "Goon Squad" Manual Teaches Officers to Violate Protesters' Rights*, Intercept (Apr. 7, 2021), https://theintercept.com/2021/04/07/nypd-strategic-response-unit-george-floyd-protests/ (detailing the NYPD's Strategic Response Group's often violent policies towards protestors).

[28] *Id.*

[29] Alex Silverman & Bill Bratton, *Court: NYPD Doesn't Have to Share Information on Secret X-Ray Vans*, CBS New York (May 11, 2016), https://newyork.cbslocal.com/2016/05/11/nypd-x-ray-van-program/.

[30] Erin Durkin, *NYC Lawmaker Pushes Bill to Make NYPD Unveil All High-Tech Surveillance Tools Used*, NY Daily News (Feb. 28, 2017), https://www.nydailynews.com/news/politics/pol-pushes-bill-nypd-unveil-high-tech-surveillance-tools-article-1.2985193.

[31] Michael Price*, Fact Check: The Post Act & National Security*, BRENNAN CTR. FOR JUST. (Mar. 6, 2017), https://www.brennancenter.org/our-work/analysis-opinion/fact-check-post-act-national-security.

[32] Ben Kochman & Erin Durkin, *NYPD Officials Argue 'Very Bad' City Council Bill Would Aid Terrorists in Working around High-Tech Surveillance Tools*, NY Daily News (Mar. 1, 2017), https://www.nydailynews.com/new-york/nypd-officials-bill-terrorists-dodge-surveillance-article-1.2986286 (reporting that NYPD deputy commissioner for legal matters stated that transparency reports required by the POST Act would end up in "the next issue of Inspire magazine," an online magazine reportedly published by al-Qaeda).

[33] Lauren Feiner, *NYC Lawmakers Pass Bill Requiring Police to Disclose Surveillance Technology*, CNBC (June 18, 2020), https://www.cnbc.com/2020/06/18/nyc-passes-bill-requiring-police-to-disclose-surveillance-technology.html ("The bill was first introduced in 2017 but has gained renewed momentum following the death of George Floyd.").

requirements starting January 2021. The POST Act requires that the NYPD provide a surveillance impact and use policy that includes a description of the capabilities of each surveillance technology used; the department's regulations and restrictions on use of such surveillance technology; security measures to protect information collected by such surveillance technology from unauthorized access; and the department's policies and practices relating to data retention, access, and use of data.[34] The NYPD is also required to disclose other entities that have access to information collected by surveillance technology (e.g., whether the data is shared with immigration agencies), whether the department requires training for individuals to use such technology, any internal oversight mechanisms within the department to ensure compliance, and any tests for the health and safety effects of the surveillance technology.[35] The NYPD's surveillance impact and use policies also must also flag potentially discriminatory behavior by identifying any disparate impacts on protected groups.[36]

III. NYPD's Draft Impact and Use Policies in Response to the POST Act

On January 11, 2021, the NYPD published draft impact and use policies for existing surveillance technologies in response to the POST Act. These policies—one per surveillance tool—purported to detail tools' capabilities, NYPD's rules on tool use and measures to prevent unauthorized use, NYPD's data retention policies, its rules on public and third-party access to data, its oversight mechanisms, and its judgment on potential discrimination (as gauged by disparate impact) due to the tools.[37] As required by law, the NYPD received feedback from the public on these drafts over a 45-day public comment period.

During the comment period, thousands of commenters expressed concerns over the lack of substance in NYPD's draft policies. Commenters remarked on the lack of disclosure of vendors' names, on incomplete information on who can access the NYPD's collected data, on NYPD's failure to meaningfully address whether tools had a disparate impact on protected groups, on missing definitions of artificial intelligence and machine learning, and more.[38] In response to a records request, S.T.O.P. received over 500 public comments filed with the NYPD on the deficiency of its draft impact and use policies. Amnesty International members reportedly submitted an additional 7,000 comments on the NYPD's draft facial recognition policy. Taken together, these comments showed that NYPD did not meet the minimal requirements of the POST Act and suggested that NYPD had not even made a good faith effort to meet its requirements.[39]

Unfortunately, the NYPD responded to this feedback by issuing final policies that largely ignored the public's feedback and that, in many cases, were not substantially different from the initial drafts. The following table summarizes NYPD's updates to its policies and indicates whether the changes were material:

[34] Public Oversight of Surveillance Technology (POST) Act, N.Y. CITY COUNCIL § 14-188 (N.Y. 2017).
[35] *Id.*
[36] *Id.*
[37] *Policies*, NYPD, https://www1.nyc.gov/site/nypd/about/about-nypd/public-comment.page (last visited July 13, 2021).
[38] *Coalition of Advocates and Academics Submit Joint Comments Documenting the NYPD's Failure to Comply with the POST Act*, BRENNAN CTR. FOR JUST. (Feb. 24, 2021), https://www.brennancenter.org/our-work/research-reports/coalition-advocates-and-academics-submit-joint-comments-documenting-nypds.
[39] *Id.*

Updates	Materiality of Update
Failed to correct errors regarding use of artificial intelligence.	**No material change.** NYPD's draft policies denied that NYPD used artificial intelligence in conjunction with certain tools, contrary to its other statements.[40] NYPD removed offending statements entirely rather than correct or clarify the record.[41]
Failed to provide more granular descriptions.	**Generally no material changes.** With few exceptions, NYPD amendments are so minor they cannot be deemed as expanding the description of the technologies' capabilities.
Failed to expand rules of use.	**Few material changes.** For most technologies, the NYPD only added that the tools may only be used "for legitimate law enforcement purposes."
Failed to expand data retention.	**Some material changes made.** NYPD amended its policies to refer to the Retention and Disposition Schedule for New York Local Government Records. But NYPD's final policies explain neither how retained data is used nor to whom access is granted.
Failed to expand safeguards and security measures.	**No substantial material changes.** NYPD added only generic language to its already-vague account of its data security practices.
Failed to disclose external entities receiving data.	**Some material changes made.** NYPD's final policies fail to identify which government agencies and third-party vendors have access to collected data or when they have access.

IV. Shortcomings of the NYPD's Implementation of the POST Act

The NYPD published its final policies on April 11, 2021. In failing to substantively respond to the public's comments, the department stripped the public of the oversight role that the POST Act set out to create. Below, we document the main substantive shortcomings of the NYPD's implementation of the POST Act. The NYPD received comments raising each of these concerns, but made no meaningful efforts to address them.

a. Vendors and product disclosures

The POST Act's "driving impetus" was the NYPD's historical failure to disclose the surveillance tools it used.[42] Commenters on the initial draft policies requested that the NYPD provide the names of the surveillance technology systems used, the systems' manufacturers, and the names of other vendors involved in the systems' creation or operation.[43] The department's final policies failed to

[40] The Legal Aid Society: Criminal Justice, *Comments on the NYPD Jan. 11, 2021 Draft Impact & Use Policies, pursuant to the Public Oversight of Surveillance Technology (POST) Act,* BRENNAN CTR. FOR JUST. (Feb. 25, 2021), https://www.brennancenter.org/sites/default/files/2021-03/Legal%20Aid%20Society%20Comments%20on%20the%20Jan.%2011%2C%202021%20NYPD%20POST%20Act%20Draft%20Policies.pdf

[41] *See, e.g., Body Worn Cameras: Impact & Use Policy,* NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/body-worn-cameras-nypd-Impact-and-use-policy_4.9.21_final.pdf "Update: Removed statement that body worn cameras do not use artificial intelligence and machine learning."

[42] Albert Fox Cahn, *supra* note 45. Albert Fox Cahn, *supra* note 45.

[43] *Id.*

include any of this information, and only describe the NYPD's programs in vague, nondescript terms.[44]

b. Data-sharing agreement

While the POST Act requires the NYPD to enumerate all entities with access to data collected by its surveillance tools, NYPD's draft policies merely stated that unspecified "agencies at the local, state, and federal level including law enforcement agencies other than the NYPD, have limited access to NYPD computer and case management systems." In response, commenters including S.T.O.P. noted that the NYPD should provide a full accounting of which agencies have access to data, how frequent their access is, and whether there are any limitations to how such data is used and retained.[45] The NYPD's final policies did not meaningfully incorporate any of these comments. In fact, identical language was carried over from draft policies to final policies and fails to enumerate which agencies have access to data.[46]

c. Racial, ethnic, and religious bias

The NYPD's draft policies failed to address the disparate impacts of its surveillance tools, even for tools with well-documented bias such as facial recognition and the Gang Database. Unfortunately, the NYPD's policies merely provide a "simple recitation of civil rights laws and antidiscrimination policies,"[47] stating,

> [t]he NYPD is committed to the impartial enforcement of the law and to the protection of constitutional rights. The NYPD prohibits the use of racial and bias-based profiling in law enforcement actions, which must be based on standards required by the Fourth and Fourteenth Amendments of the U.S. Constitution, Sections 11 and 12 of Article I of the New York State Constitution, Section 14-151 of the New York City Administrative Code, and other applicable laws. Race, color, ethnicity, or national origin may not be used as a motivating factor for initiating police enforcement action.

This language fails to meaningfully address the NYPD's long-documented, technology-facilitated bias and discrimination against communities of color.[48] The POST Act provided the NYPD with the opportunity to address how its surveillance is influenced by and compounds discrimination.[49]

[44] *See, e.g.*, *Criminal Group Database: Impact & Use Policy*, (Apr. 11, 2021), *supra* note 56 (neglecting to name any equipment, software, contractor, or vendor).

[45] *See, e.g.,* Albert Fox Cahn, *Re: S.T.O.P. Comment on NYPD's Draft Criminal Group Database Impact & Use Policy*, SURVEILLANCE TECH. OVERSIGHT PROJECT (Feb. 25, 2021), https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/603964bff52b47437dbcabb5/1614374079596/2021-02-25_Criminal_Group_Comment.pdf.

[46] *Criminal Group Database: Impact & Use Policy* (Apr. 11, 2021), *supra* note 56.

[47] *Coalition of Advocates and Academics Submit Joint Comments Documenting the NYPD's Failure to Comply with the POST Act*, *supra* note 39 at 1.

[48] *See* Lauren del Valle, *supra* note 23.

[49] *See, e.g.*, Alex Najibi, *Racial Discrimination in Face Recognition Technology*, Science in the News (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ (citing discriminatory law enforcement practices of the NYPD); *Factsheet: The NYPD Muslim Surveillance Program*, ACLU, https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program (last visited Aug. 17, 2021); Clare Garvie, Alvaro Bedoya, & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Geo. L. Ctr. on

Instead, the draft polices ignored patterns of bias and merely state that "[t]he NYPD prohibits the use of racial and bias-based profiling in law enforcement actions," in direct conflict with well-established precedent. Though multiple commenters pointed this out during the public comment period,[50] the NYPD's final text on disparate impact mirrors the draft text verbatim.

d. Retention periods and access rights

The POST Act requires the NYPD to clarify how long data collected by surveillance technology is stored and who *within* the NYPD has access to this data. This requirement is distinct from the reporting requirement regarding external entities with whom the NYPD shares its data, such as federal or state law enforcement agencies.[51] Yet the NYPD's draft policies only featured "boilerplate language"[52] stating that data would be retained "in accordance with applicable laws, regulations, and New York City and NYPD policies."[53] NYPD didn't even disclose the kinds of information that its tools collect.[54]

In response to comments identifying these deficiencies, the NYPD purportedly "added language to reflect NYPD obligations under federal, state, and local record retention laws."[55] However, much of this new language—beyond recapitulating the Retention and Disposition Schedule for New York Local Government Records—is vague and at times nonsensical. One bit of incoherent final policy language states that "[p]ersonal information data files on associated persons, such as victims, relatives and witnesses must be retained as long as, or information as part of relevant case investigation record [sic]."[56]

e. NYPD data security

The NYPD described its data security practices using vague, boilerplate language. The initial draft policies merely stated that the department uses a "multifaceted approach to secure data and user accessibility."[57] As S.T.O.P. wrote in its comment on NYPD's draft facial recognition policy, this

PRIVACY & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/ (documenting how police facial recognition disproportionately affects Black individuals); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROCEEDINGS OF MACHINE LEARNING RESEARCH 1, 11 (2018) (finding facial recognition technology misclassification worse on female subjects than male subjects and on darker subjects than lighter subjects).

[50] *See, e.g.*, *Coalition of Advocates and Academics Submit Joint Comments Documenting the NYPD's Failure to Comply with the POST Act*, supra note 39 at 1; Albert Fox Cahn, *Re: S.T.O.P. Comment on NYPD's Draft Criminal Group Database Impact & Use Policy*, *supra* note 45.

[51] *Compare* Public Oversight of Surveillance Technology (POST) Act, N.Y. CITY COUNCIL § 14-188.4 (N.Y. 2017) (requiring surveillance impact and use policy to include "policies and/or practices relating to the retention, access, and use of data collected by such surveillance technology"), *with* Public Oversight of Surveillance Technology (POST) Act, N.Y. CITY COUNCIL § 14-188.6 (N.Y. 2017) (requiring surveillance impact and use policy to include "whether entities outside the department have access to the information and data collected by such surveillance technology").

[52] *Id.*

[53] *Criminal Group Database: Impact & Use Policy* (Apr. 11, 2021), *supra* note 56.

[54] *Comply with the POST Act*, BRENNAN CTR. FOR JUST., at 3 (Feb. 24, 2021) https://www.brennancenter.org/our-work/research-reports/coalition-advocates-and-academics-submit-joint-comments-documenting-nypds.

[55] *Facial Recognition: Impact & Use Policy*, NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/facial-recognition-nypd-impact-and-use-policy_4.9.21_final.pdf..

[56] *Id.*

[57] *Id.*

description is "so generic that it is almost completely useless from a technical standpoint."[58] The technical mechanisms that NYPD did specify—its use of Lightweight Directory Access Protocol, dual factor authentication, Secure Socket Layer, and Transport Layer Security—are so "rudimentary" and "ubiquitous" that "it would only be notable if they were not used as part of the NYPD's data security policy."[59]

Once again, NYPD did not respond to these comments in its final policies. Aside from adding, unhelpfully, that the "NYPD maintains an enterprise architecture (EA) program, which includes an architecture review process to determine system and security requirements on a case by case basis,"[60] NYPD made no material changes to its data security policies.

f. NYPD training

Commenters described the NYPD's draft policies on officer training as grossly insufficient and uninformative. For instance, the NYPD's draft policy for facial recognition technology merely stated that NYPD employees given access to facial recognition technology must complete a "mandatory training related to use of the technology" and that "NYPD personnel utilizing facial recognition technology receive specialized training on the proper operation of the technology and associated equipment. NYPD personnel must use facial recognition technology in compliance with NYPD policies and training."[61] Given the NYPD's repeated abuses of its technologies,[62] the draft policy failed to provide information on whether officers knew what constituted abuse of facial recognition or whether the NYPD implicitly condoned and perpetuated misuse by failing to provide meaningful training to its officers. The NYPD did not update this language in its final policy.[63]

g. Inconsistency with other NYPD policies

At least once, NYPD even contradicted its own written policies in its POST Act reporting. NYPD's draft facial recognition policy stated that "[t]he NYPD does not use facial recognition technology to monitor and identify people in crowds or political rallies."[64] Commenters pointed out that there have been documented instances to the contrary[65] and that the policy was inconsistent with advice in

[58] Albert Fox Cahn, *Re: S.T.O.P. Comment on NYPD's Draft Facial Recognition Impact & Use Policy,* SURVEILLANCE TECH. OVERSIGHT PROJECT (Feb. 23, 2021), https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/603963cd31f3472a75b2b029/1614373837179/2021-02-23_Facial+Recognition_STOP+Organizational+Comment+FINAL.pdf; see also Stevie DeGroff & Albert Fox Cahn, New CCOPS on The Beat, SURVEILLANCE TECH. OVERSIGHT PROJECT, at 10 (Feb. 10, 2021), https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/602430a5ef89df2ce6894ce1/1612984485653/New+CCOPS+On+The+Beat.pdf ("Other jurisdictions submit opaque or boiler-plate responses, hiding the details needed for meaningful public engagement.").

[59] Albert Fox Cahn, *supra* note 58.

[60] *Facial Recognition: Impact & Use Policy*, NYPD (Jan. 11, 2021).

[61] *Id.*

[62] *See supra* Section II.a (detailing various concerning NYPD practices leading to the passage of the POST Act).

[63] *Id.* ("Facial recognition investigators are provided with access only after completing mandatory training related to use of the technology."); *id.* ("NYPD personnel utilizing facial recognition technology receive training on facial recognition technology, image comparison principles, the proper operation of the technology and associated equipment. NYPD personnel must use facial recognition technology in compliance with NYPD policies and training.").

[64] *Id.*

[65] Albert Fox Cahn, *supra* note 58 (recounting how bystander photos indicate that one NYPD officer was holding a facial recognition report from the department's Facial Identification Section during a standoff with a political organizer).

NYPD's own Patrol Guide. NYPD did not correct its language in its final facial recognition policy.[66]

V. The NYPD's POST Act Compliance Compared to other U.S. Police Agencies Compliance with Comparable Laws

Unsurprisingly, the NYPD's implementation of the POST Act falls short of the reporting standards of other U.S. police agencies bound by comparable surveillance oversight measures. For instance, in all but two of the NYPD's final impact and use policies (body worn cameras and ShotSpotter), the NYPD fails to identify a single vendor for the surveillance technologies it uses. NYPD also fails to provide a single make or model of any of its surveillance tools. In stark contrast, the Seattle Police Department has provided specific vendors and models of technology.[67]

The NYPD also fails to specify the number of vendors that receive data through its use of surveillance technology. Rather, in each impact and use policy, NYPD states that "[v]endors and contractors may have access" to surveillance technology "associated with software or data in performance of contractual duties to the NYPD."[68] But the NYPD fails to disclose how many third party entities have access, and which ones have access. By contrast, the Berkeley Police Department discloses each of the vendors with which it will share data.[69] Similarly, the City Manager of Cambridge, Massachusetts prepares an Annual Surveillance Report to the City of Cambridge[70] that identifies the city's surveillance technology vendors and the third-party entities with which it shares data collected by each technology.[71]

Finally, with few exceptions, the NYPD fails to provide specific data retention periods for its surveillance technologies.[72] In most cases, the NYPD provided identical, boilerplate language that

[66] *Facial Recognition: Impact & Use Policy* (Apr. 11, 2021), *supra* note 55.

[67] *See, e.g.,* Seattle Police Department, *Forward Looking Infrared Real-Time Video (FLIR) (KCSO Helicopters),* SEATTLE INFORMATION TECH. (2020), https://www.seattle.gov/Documents/Departments/Tech/Privacy/FLIR%20-%20KCSO%20Helicopters%20WG%20SIR.pdf (listing the specific models and makes of its helicopters); Seattle Police Department, *Automated License Plate Recognition* (ALPR) (Patrol), SEATTLE INFORMATION TECH. (Jan. 31, 2019), https://www.seattle.gov/Documents/Departments/Tech/Privacy/SPD%20ALPR%20(Patrol)%20-%20Final%20SIR.pdf (identifying vendor of software); Seattle Police Department, *CopLogic*, SEATTLE INFORMATION TECH. (2019), https://www.seattle.gov/Documents/Departments/Tech/Privacy/SPD%20CopLogic%20Final%20SIR.pdf (identifying specific software and vendor of surveillance technology).

[68] *See, e.g., Audio-Only Recording Devices, Covert: Impact and Use Policy,* NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/audio-only-recording-devices-covert-nypd--impact-and-use-policy_4.9.21_final.pdf.

[69] Berkeley Police Department, *Surveillance Use Policy – Body Worn Cameras,* CITY OF BERKELEY (Feb. 25, 2021), https://www.cityofberkeley.info/uploadedFiles/Police/Level_3_-_General/Surveillance_Use_Policy_-_Body_Worn_Cameras.pdf..

[70] Chapter 2.128 - Surveillance Technology Ordinance, CAMBRIDGE, MASS. CODE OF ORDINANCES (Dec. 10, 2018), https://library.municode.com/ma/cambridge/codes/code_of_ordinances?nodeId=TIT2ADPE_CH2.128SUTEOR.

[71] *Annual Surveillance Report*, CITY OF CAMBRIDGE (Feb. 28, 2020), https://www.cambridgema.gov/-/media/Files/citymanagersoffice/surveillanceordinancedocuments/secondannualsurveillancereports_combined22820.pdf..

[72] Closed circuit television systems, manned aircraft systems, and unmanned aircraft systems have a standard retention period of 30 days, subject to exception through the Retention and Disposition Schedule for New York Local Government Records. *Closed-Circuit Television Systems: Impact and Use Policy*, NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/cctv-systems-nypd-Impact-and-use-policy_4.9.21_final.pdf; *Manned Aircraft Systems: Impact and Use Policy*, NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/manned-aircraft-systems-nypd-impact-and-use-policy_4.9.21_final.pdf; *Unmanned Aircraft Systems: Impact and Use Policy*, NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/unmanned-aircraft-systems-uas-nypd-impact-and-use-policy_4.9.21_final.pdf. ShotSpotter has a retention period of 30 hours, subject through the Retention and Disposition

the retention period "depends on the classification of a case investigation record" subject to the Retention and Disposition Schedule for New York Local Government Records. This Schedule establishes the minimum length of time local government agencies must retain their records before the records may be legally disposed depending on the type of offense. NYPD does not clarify, for example, how long data is retained when an individual is not convicted or does not plead to an offense. In contrast, the Berkeley, California Police Department provides far more concrete data retention policies. For example, in its use policy for body worn cameras, the Berkeley Police Department it specifies a minimum retention period of 60 days, with different minimum retention periods based on the type of incident.[73] It also explains when data or recordings are deleted—at the same time as other evidence following the full adjudication of a matter.[74]

VI. Conclusion

NYPD's impact and use policies fall short of satisfying the requirements of the POST Act. They fall short of comparable police agencies' implementations of oversight requirements in other municipalities.

While lawmakers created the POST Act in response to serious privacy concerns stemming from technology used by law enforcement, the Act's implementation does little to actually address those concerns. Additionally, the NYPD's impact and use policies fall short and do not inspire much hope that the Department will make a good-faith effort to comply with the POST Act. Indeed, serious concerns with the POST Act that the public raised during the public comment period were not addressed in the language contained in the final policies. Finally, the NYPD's implementation of the POST Act is much weaker than other departments' responses to CCOPS legislation around the country.

At a minimum, the New York City Council must use its oversight authority to ensure that the bill it fought so long to implement is not ignored. NYPD officials need to be held accountable for their willful disregard for the law. Additionally, individual lawmakers and civil society organizations can continue to evaluate potential litigation, seeking judicial intervention to compel the NYPD to comply with both the letter and the intent of the POST Act.

Schedule for New York Local Government Records. *ShotSpotter: Impact and Use Policy*, NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/shotspotter-nypd-impact-and-use-policy_4.9.21_final.pdf. License plate readers have a standard retention rate of 5 years, subject to exception through the Retention and Disposition Schedule for New York Local Government Records. *License Plate Readers: Impact and Use Policy*, NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/license-plate-readers-lpr-nypd-impact-and-use-policy_4.9.21_final.pdf.

[73] Berkeley Police Department, *Surveillance Use Policy – Body Worn Cameras*, CITY OF BERKELEY (Feb. 25, 2021), https://www.cityofberkeley.info/uploadedFiles/Police/Level_3_-_General/Surveillance_Use_Policy_-_Body_Worn_Cameras.pdf.

[74] *Id.*

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT

Surveillance Technology
Oversight Project, Inc.

40 Rector Street
9th Floor
New York, NY 10006
www.STOPSpying.org