New York City
Department of Investigation

Office of the Inspector General for the NYPD (OIG-NYPD)

# An Assessment of NYPD's Response to the POST Act

Jocelyn Strauber
Commissioner

Jeanene Barrett
Acting Inspector General for the NYPD

November 2022

## Table of Contents

## I. Executive Summary

The New York City Police Department ("NYPD") conducts widespread surveillance in the public domain using data gathered by sophisticated technology throughout New York City.[1] That technology has the capability to gather information about millions of people who move around the City. Examples of the technologies include License Plate Readers ("LPRs") and Facial Recognition Technology ("FRT"). Cars that travel from Queens to Manhattan pass dozens of Automated LPRs, which take a snapshot of a car's license plate at particular locations and times, enabling authorities to later approximate a vehicle's route. Subway passengers traveling in Manhattan from Uptown to Midtown pass hundreds of surveillance video cameras, which collect images that can later be processed by FRT. These are just two of the many types of surveillance technologies that generate data that can be used and accessed by NYPD.

These powerful law enforcement tools can play an important role in protecting public safety and aiding law enforcement in the search for missing persons or individuals suspected of committing crimes, but under certain circumstances their use may infringe on significant public rights. Therefore, sound policies and robust oversight are necessary to ensure that the capacities of these law enforcement technologies are not misused and to assure the public that these tools are being used appropriately.

Advocacy groups and community organizations across New York City have expressed concern about the Department's use of surveillance technologies.[2] Those concerns

* DOI Commissioner Jocelyn Strauber and Acting Inspector General Jeanene Barrett thank the staff of OIG-NYPD for their efforts in producing this Report, specifically, Justyn Richardson, Assistant Inspector General; Percival Rennie, Deputy Inspector General – Policy; Tyler Gibson, Senior Attorney; and Julie Marling, Investigative Attorney. Appreciation is extended to the New York City Police Department and representatives of other organizations for their assistance and cooperation during this investigation.

Special thanks are given to the former OIG-NYPD team members who contributed to the advancement of this investigation: Renell Grant and Kevonte M. Mitchell.

[1] The surveillance technologies discussed in this Report include technologies owned, operated, and maintained by other entities, such as the Department of Transportation (with respect to License Plate Readers) or the Metropolitan Transit Authority (with respect to subway surveillance cameras), which generate data to which the NYPD has access.
[2] *See, e.g.*, Albert Fox Cahn, *20 Years After 9/11, Surveillance Has Become a Way of Life*, WIRED (Sept. 9, 2021).

principally relate to the technologies' impact on civil liberties, reduced privacy in public spaces, the risk of racially targeted monitoring, and NYPD's potentially unauthorized retention of individuals' identifying data. The available equipment — including aerial drones, surveillance towers, and social media monitoring software — enables the Department to observe a range of public activity, including conduct that is political in nature.[3] Some surveillance technologies lawfully and automatically capture information about individuals who are not suspected of criminal activity and are not involved in any criminal conduct. Concerns about potential use of information obtained through this type of surveillance has fueled distrust of NYPD, particularly among communities of color and certain religious groups.[4]

To provide public oversight of the use of this technology, and to promote transparency with respect to NYPD's use of surveillance technology, on June 18, 2020, New York City Council passed the Public Oversight of Surveillance Technology (POST) Act requiring "comprehensive reporting and oversight of New York City Police Department surveillance technologies."[5] Among other directives, the POST Act requires NYPD to produce and publish Impact and Use Policies ("IUPs") for each of its qualifying surveillance technologies.[6]

https://www.wired.com/story/20-years-after-911-surveillance-has-become-a-way-of-life/.

[3] Aerial drones are typically small, unmanned, remote-controlled flying machines capable of being outfitted with cameras, microphones, and other surveillance technologies. Surveillance Towers are mobile surveillance towers parked in public areas, which allow officers to monitor areas from several stories above street level as well as record movements within a targeted area. Social media monitoring software/Social Network Analysis Tools are software capable of monitoring social media content (e.g., posts, pictures, "likes") according to keywords or relationship to a target individual. For further information on the above technologies, see Angel Diaz, *New York City Police Department Surveillance Technology*, BRENNAN CTR. FOR JUSTICE (Oct. 4, 2019), https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology.

[4] *See, e.g.*, Matt Katz, *NYPD's Legacy of Police Surveillance, From Black Panthers to Mosques to Black Lives Matter*, GOTHAMIST (Sept. 7, 2021), https://gothamist.com/news/nypds-legacy-of-police-surveillance-from-black-panthers-to-mosques-to-black-lives-matter; Zainab Iqbal, *After Decades of Surveillance, Muslims Struggle With How Much to Share Online: The Long Shadow of NYPD Surveillance After 9/11*, THE VERGE (Dec. 7, 2021), https://www.theverge.com/22810372/muslim-surveillance-social-media-nypd-new-york-informants-mosque.

[5] Creating Comprehensive Reporting and Oversight of NYPD Surveillance Technologies (POST Act), N.Y.C. Local Law No. 65 (2020) (codified at N.Y.C ADMIN. CODE § 14-188 and N.YC. CHARTER § 803[c-1]).

[6] See Appendix A for the relevant POST Act language, including with respect to the IUP requirements.

The POST Act requires, among other things, that the IUPs describe the capabilities of surveillance technology, and include any rules, processes, and guidelines that regulate access to or use of the technology, and any prohibitions or restrictions on its use, and any potential disparate impacts. The POST Act mandates that the Department publish draft IUPs on its website within 180 days of the effective date of the law (i.e., no later than January 11, 2021) for existing surveillance technologies, and at least 90 days prior to the use of any new surveillance technology.

The POST Act gives the Department of Investigation's ("DOI") Office of the Inspector General for the NYPD ("OIG-NYPD") oversight responsibility to ensure that NYPD complies with its policies on surveillance technology use. The Act directs that OIG-NYPD prepare annual audits of NYPD's use of surveillance technologies that:

1. Assess whether NYPD's use of surveillance technologies complies with published IUPs;

2. Describe any known or reasonably suspected violations of the IUPs; and

3. Publish recommendations, if any, relating to revisions of any IUPs.

OIG-NYPD reviewed the IUPs posted by NYPD on April 11, 2021 and determined that it could not conduct the type of audit required by items 1 and 2 above for this Report.[7] As explained throughout this Report, the vast majority of the IUPs produced by NYPD were general and generic in part (in that similar language was used in many of the IUPs) making it impracticable for OIG-NYPD to meaningfully assess the Department's compliance with all of its IUPs. Instead of an audit, this Report makes a number of recommendations relating to revisions to the IUPs (item 3 above) that will facilitate the mandated audits in the future.

In connection with its preparation of this Report, OIG-NYPD (1) interviewed a range of individuals including NYPD officials, supporters of the Act, and experts on various surveillance technologies; (2) reviewed all published IUPs and performed a section-by-section assessment of one IUP; (3) conducted an in-depth assessment of two selected surveillance technologies and the related IUPs; and (4) researched the rules applicable in other jurisdictions with respect to surveillance technologies, to better

[7] *See Public Oversight of Surveillance Technology (POST) Act Impact and Use Policies*, N.Y.C. POLICE DEP'T., https://www1.nyc.gov/site/nypd/about/about-nypd/policy/post-act.page (last visited Nov. 1, 2022).

understand other approaches to transparency concerning the nature and use of such technologies.

From this assessment, OIG-NYPD found that:

- NYPD has largely complied with the POST Act legislation with respect to the issuance of IUPs. That is, NYPD has issued IUPs that describe the capabilities of surveillance technologies and include the other categories of information that the POST Act requires. However, based on its investigation, the Office finds that merely meeting these requirements of the POST Act is insufficient to enable OIG-NYPD to conduct full annual audits (as the Act also requires) and to achieve appropriate transparency with the public, consistent with practices in other jurisdictions, as to the nature and use of these technologies.

- The IUPs included, in many relevant parts, boilerplate language that failed to provide sufficient detail concerning the use or nature of the technology at issue, or to differentiate between technologies. For example, NYPD used general language, much of which was identical, to address access to data and data retention for various technologies, which did not clearly identify, among other things, the specific agencies with access to the data or the length of time such data would be retained by NYPD.

- The POST Act's language requires IUPs to include "any potentially disparate impacts of the surveillance technology *[I]mpact and [U]se [P]olicy* on any protected groups as defined in the New York City [H]uman [R]ights [L]aw [emphasis added]." Because the Act requires the IUP to address only the disparate impact of the policy, rather than *the disparate impact of the technology*, the Act does not ensure that NYPD will publicly disclose any disparate impact of the technology itself. While NYPD largely complied with the Act's limited requirements concerning disclosure of the disparate impact of the IUPs, and in 5 out of 36 IUPs (14%) went beyond these requirements by addressing the potential disparate impact of the *use of the technology*, NYPD did not provide such information with respect to the vast majority of the IUPs.[8]

[8] Some potential disparate impacts of the use of the technology are presented in the IUPs for Facial Recognition Technology, Criminal Group Database, Mobile X-Ray Technology, Data Analysis Tools, and Shotspotter (*see Public Oversight of Surveillance Technology (POST) Act Impact and Use Policies*, *supra* note 7).

- NYPD grouped related technologies and issued a single IUP for multiple technologies. This approach significantly limits the information made available to the public concerning the nature and use of individual technologies (to the extent grouped technologies differ). NYPD informed OIG-NYPD that time constraints and operational considerations contributed to this approach. Furthermore, NYPD takes the position that the functionality of many of the technologies are the same, such that individual IUPs are unnecessary, and claims that the Act does not require an inventory of every technology. It is OIG-NYPD's position that the POST Act does in fact require an IUP for each surveillance technology. NYPD's interpretation, which allows grouping of several technologies under a single IUP, is contrary to the intent of the POST Act.

- It is OIG-NYPD's position that the most logical reading of the POST Act's language is that it requires an IUP for each surveillance technology. Moreover, NYPD's interpretation of the POST Act that permits grouping significantly undermines other requirements of the Act. For example, grouping may enable NYPD to bypass the POST Act's disclosure requirements for new technologies. That is, NYPD's grouping approach allows it to introduce new technologies under an existing group category covered by an existing IUP, and begin use immediately without the required notification to the public and City Council. This allows NYPD to avoid the public notification process – a critical aspect of the POST Act – and thus cannot have been the intent of the legislation.

- NYPD's grouping of related technologies also poses a practical barrier to OIG-NYPD's ability to fulfill its duties under the POST Act. Although the Department provided OIG-NYPD access to its list of technologies, the list did not include information concerning the functionality/capability of each technology — information necessary to assess whether the technologies might appropriately be grouped and whether NYPD is actually issuing IUPs with respect to each functionality and capability. Furthermore, without more information about the functionalities of the various technologies, OIG-NYPD cannot assess whether NYPD's use of surveillance technologies complies with published IUPs. For instance, the "DigiDog" robot— deployed as part of a pilot program by NYPD— has significant capabilities that potentially overlap with multiple IUP groups. It is unclear, from an oversight perspective, which IUP(s) govern the use of this technology, and, if more than one, which aspect of each IUP applies to this robotic device. This lack of clarity underscores the need for an IUP for each specific technology.

Based on these and other findings, OIG-NYPD makes the following recommendations:

1. NYPD should issue an IUP for each individual surveillance technology, as opposed to continuing its practice of grouping similar technologies under a single IUP.

2. NYPD should identify in each IUP each external agency, by name, with which the Department can share surveillance data.

3. NYPD should include in each IUP the specific safeguards/restrictions on use or dissemination of the surveillance data, for each external agency with which the Department can share such data.

4. NYPD should include in each IUP the potential disparate impacts on protected groups of the use and deployment of the surveillance technology itself.

5. NYPD should revise the Health & Safety Reporting sections of all published IUPs, to include any safety hazards that are identifiable on the basis of existing research, manufacturer warnings, or evaluations by experts in the field, or to state that no such hazards have been identified after a search for relevant information.

6. Within 180 days, NYPD should convene a working group of NYPD personnel, relevant City Council members or their appointees, and representatives from select advocacy groups and community organizations who have expertise in surveillance technologies. The purpose of the working group is to make recommendations to NYPD on necessary updates to the existing IUPs and on any information that should be included in any future IUPs for new technologies, based on the group's expertise. NYPD's procedures applicable to the working group should ensure the protection of sensitive information as appropriate.

7. Within 180 days, NYPD should create an internal tracking system for every instance in which NYPD provides an external agency with data collected via surveillance technologies that NYPD controls, including the name of the agency and the date of that the data was provided.

8. Within 90 days, in order to facilitate OIG-NYPD's statutorily obligated audit under the POST Act, NYPD should provide OIG-NYPD with information indicating, for each surveillance technology, the various types of data collected and which NYPD units maintain that information. NYPD should include

information about the retention procedures and practices for each type of data collected so that OIG-NYPD can assess NYPD's compliance with the IUPs.

9. NYPD should provide OIG-NYPD with any data access and retention policies that are included in the existing contracts with vendors who supply the surveillance technologies used by NYPD.

10. NYPD should provide OIG-NYPD with the data access and retention policies contained in any newly executed contracts with surveillance technology vendors by the 15th of each quarter (i.e., January, April, July, and October).

11. Within 30 days, NYPD should provide OIG-NYPD an itemized list of the surveillance technologies that it uses. This list should include information concerning the functionalities of each technology, so that OIG-NYPD can assess whether NYPD has, in fact, issued an IUP that covers each surveillance technology that has a distinct functionality or capability.

12. NYPD should create written policies establishing guidelines to specify the modifications that can be made to probe images used for Facial Recognition Technology.

13. NYPD should conduct periodic audits of its Facial Identification Section's use of facial recognition technology to ensure compliance with its policies related to the use of the technology and its data. This auditing process should be memorialized in writing.

14. To facilitate the OIG-NYPD's mandated annual audits, beginning January 15, 2023, NYPD should provide OIG-NYPD with quarterly updates, reflecting newly acquired or discontinued technologies in an itemized list of the surveillance technologies that it uses. Thereafter, updates should be made available by the 15th of each quarter (i.e., January, April, July, and October).

15. NYPD should issue a press release announcing the publication, related public comment period of any new IUPs, and subsequently publish the press release on its website.

## II. Introduction and Background

On July 15, 2020, then-Mayor Bill de Blasio signed the Public Oversight of Surveillance Technology ("POST") Act into law.[9] The measure, New York City's adaptation of the Community Control over Police Surveillance ("CCOPS") model, requires NYPD to publicly disclose information concerning its surveillance technology and to develop policies on the use of those tools.[10]

The POST Act defines surveillance technology as "equipment, software, or systems capable of, used or designed for, collecting, retaining, processing, or sharing audio, video, location, thermal, biometric, or similar information, that is operated by or at the direction of [NYPD]."[11] For each qualifying technology, NYPD must publish an Impact and Use Policy ("IUP") that reports on the following ten areas (see Appendix A for a copy of the relevant portion of the statute):

1. A description of the capabilities of the technology;

2. Rules, processes, and guidelines issued by NYPD regulating access to or use of the technology, including whether NYPD obtains court authorization for use;

3. Safeguards designed to protect information collected by the technology from unauthorized access;

4. Policies and/or practices relating to law enforcement's retention, access, and use of data collected by the technology;

[9] POST Act, s*upra* note 5.

[10] The Community Control Over Police Surveillance (CCOPS) model provides a template for legislation in the United States (*Community Control over Police Surveillance (CCOPS) Model Bill,* AMERICAN CIVIL LIBERTIES UNION, https://www.aclu.org/legal-document/community-control-over-police-surveillance-ccops-model-bill (last updated April 2021). Introduced by the American Civil Liberties Union (ACLU), the model aims to improve communities' ability to review and control law enforcements' use of surveillance technologies. It has served as a model for similar legislation enacted around the country (*Community Control Over Police Surveillance (CCOPS)*, AMERICAN CIVIL LIBERTIES UNION, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance?redirect=feature/community-control-over-police-surveillance [last visited Nov 1, 2022]).

[11] POST Act, *supra* note 5.

5. Policies and procedures relating to access or use of data collected by the technology by members of the public;

6. Details about whether outside entities have access to the data collected by the technology;

7. Information regarding any training that NYPD requires for individuals to use the technology;

8. A description of internal audit and oversight mechanisms to ensure compliance with the IUPs;

9. Any tests or reports regarding the health and safety effects of the technology; and

10. Any potential disparate impacts "of the surveillance technology [I]mpact and [U]se [P]olicy" on any protected groups as defined by NYC Human Rights Law.[12]

The Act requires NYPD to publish draft IUPs for its existing surveillance technologies for public comment within 180-days from the date of enactment.[13] It also requires NYPD to publish an IUP on its website at least 90 days prior to the use of any new surveillance technologies; Figure 1 illustrates this process. After publication, for both existing and new technologies, the public has 45 days to submit comments. NYPD then has an additional 45 days to publish the final IUPs on its website.

Consistent with the requirements of the Act, on January 11, 2021, NYPD published 36 draft IUPs on its website, 180 days after the signing of the POST Act.[14] The posted policies remained open 45 days for public comments to be uploaded directly through its website. NYPD did not issue a press release announcing the posting or the public comment period, which the Act does not require.

[12] *Id.*

[13] This 180-day deadline corresponded to the end of January 2021.

[14] *Draft Policies for Public Comment*, N.Y.C. POLICE DEP'T., https://www1.nyc.gov/site/nypd/about/about-nypd/public-comment.page [https://perma.cc/AV44-UJHL?type=image].

NYPD received 7,819 public comments on the IUPs during the 45-day period from January 11, 2021 through February 25, 2021. Of those, 7,392 comments (95%) were identified by the Department as potential spam. NYPD informed OIG-NYPD that the remaining 5% of the comments on the IUPs were identical. According to the Department, those comments were sent via the websites of two advocacy groups, Amnesty International and Surveillance Technology Oversight Project (STOP), that provided a pre-filled template concerning the draft IUPs for submission.[15]

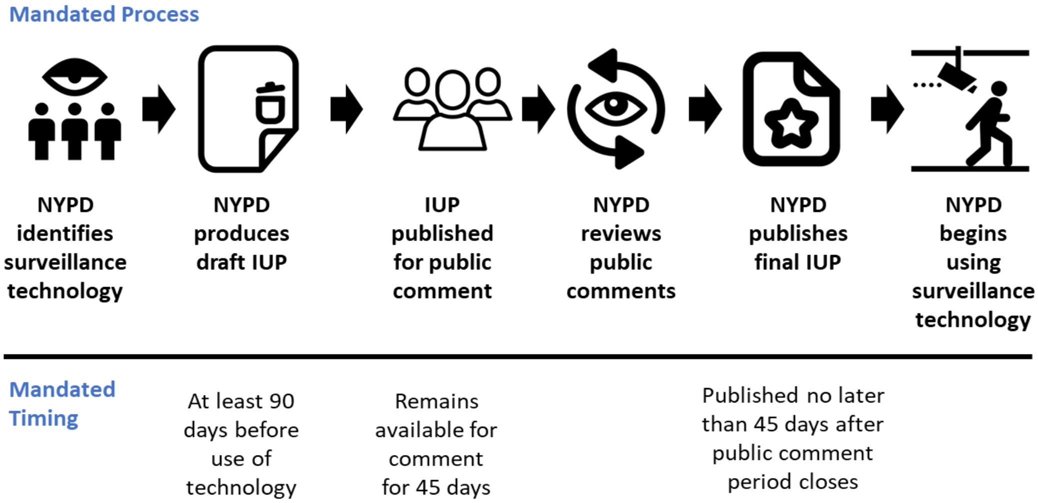
In interviews, members of the Department explained that during the above-mentioned 45-day period, the public comments were reviewed by a three-person team of NYPD attorneys in order to determine whether any changes would be made. A summary of the changes made to the draft policies appears on the first page of the IUPs. As an example, for the two IUPs that are analyzed in this Report – Facial Recognition and Social Analysis Network Tools – the public comments highlighted that there is no industry-standard definition for "artificial intelligence" and "machine learning" (terms used in the draft IUPs). The POST Act does not require that NYPD comment on whether the technologies include such functionalities, nor does it require that these terms be defined. In the final IUP, NYPD did not include a definition of these terms, but instead removed them entirely. While not in violation of the POST Act, this change heightened public suspicion that the Department's IUPs were not transparent with respect to the surveillance technologies' functionalities.[16]

**Figure 1: Mandated Process for New Surveillance Technology as Defined by the POST Act Legislation**[17]

[15] See Appendix B for an example of this pre-filled template.

[16] *See* Michael Sisitzky, & Ben Schaefer, *The NYPD Published Its Arsenal of Surveillance Tech. Here's What We Learned,* ACLU of N.Y. (Feb. 24, 2021), https://www.nyclu.org/en/news/nypd-published-its-arsenal-surveillance-tech-heres-what-we-learned.

[17] POST Act legislation graphic created by OIG-NYPD staff.


Mandated Process
NYPD identifies surveillance technology
NYPD produces draft IUP
IUP published for public comment
NYPD reviews public comments
NYPD publishes final IUP
NYPD begins using surveillance technology
Mandated Timing
At least 90 days before use of technology
Remains available for comment for 45 days
Published no later than 45 days after public comment period closes

## III. The POST Act's Requirements and Community Expectations

The POST Act directs the Office of the Inspector General for the NYPD ("OIG-NYPD") to publish any recommendations relating to the revision of IUPs. Aside from some gaps in compliance discussed herein, OIG-NYPD has concluded that NYPD has largely complied with the limited requirements of the POST Act. However, it is OIG-NYPD's position that NYPD can and should provide greater transparency than the POST Act requires, with respect to the technologies it employs, without disclosing sensitive law enforcement information that might compromise public safety. The Office's position with respect to the need for greater transparency is principally based on community expectations, the practices of other jurisdictions with respect to surveillance technologies, and the City's practices with respect to public involvement in rulemaking in other areas.

### A. The POST Act Imposes Limited Requirements

As noted above, the POST Act's requirements are limited. The Act directs NYPD to, at a minimum, publish information on its surveillance technologies in the required ten areas within the mandated time period. For existing technologies, the Department published draft IUPs, allowed requisite time for public comment, and thereafter published final drafts, all within the required time periods. Each IUP included information for each of the ten required areas. NYPD therefore has largely complied with this limited requirement of the POST Act, with certain specific exceptions discussed further herein.[18] OIG-NYPD's recommendations, as noted above, are based on its determination that additional transparency would better serve the public and be consistent with the practices in other jurisdictions.

### B. The POST Act as Enacted Failed to Meet Some Community Expectations

This investigation concluded that the POST Act did not require the same level of transparency with respect to the use of surveillance technology as other jurisdictions require, and as advocates involved in the passage of the Act expected. A review of comparable legislation in other jurisdictions, New York City practice with respect to proposed rulemaking in other contexts, and interviews of advocates support this conclusion.

#### 1. Surveillance Technology Oversight Legislation

To better inform OIG-NYPD's understanding of the initial objectives of the POST Act, the Office reviewed surveillance technology oversight legislation from around the country.[19] This review revealed similar legislation in at least seven states and nearly two dozen cities: some requiring other administrative agencies or working groups to assist with the creation, review, and approval of surveillance technology policies; some requiring an opportunity for public comment during properly noticed public meetings; and some giving separate administrative bodies, or City Councils, the authority to approve or reject acquisitions of surveillance technologies. See Figure 2 for an example process from Seattle.

In contrast to all other city ordinances reviewed, New York City's POST Act requires that NYPD disclose only basic details about the technology that is being deployed. For example, the Seattle Police Department's ("SPD's") Surveillance Impact Report on License Plate Readers ("LPRs"), which is comparable to an IUP, is 353 pages and

[18] There are some gaps in compliance, especially with regard to NYPD's practice of grouping multiple technologies within a single IUP. See Section VII.C below.

[19] The Office conducted a more in-depth comparative analysis of legislation from Santa Clara County, and San Francisco, California as well as Seattle, Washington, locations with population, urban density and security threats comparable to New York City's.
SANTA CLARA CNTY., CAL., CODE OF ORDINANCES § A40-1 to A40-12 (2016), http://sccgov.iqm2.com/Citizens/FileOpen.aspx?Type=4&ID=149330&MeetingID=7193;
SEATTLE, WASH., MUN. CODE 14.18.010-18.080 (2018), https://library.municode.com/wa/seattle/codes/municipal_code?nodeId=TIT14HURI_CH14.18ACUSSUTE_14.18.010DE;
S.F., CAL., ADMIN. CODE Ch. § 19B.1-B.10 (2019), https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-47320.

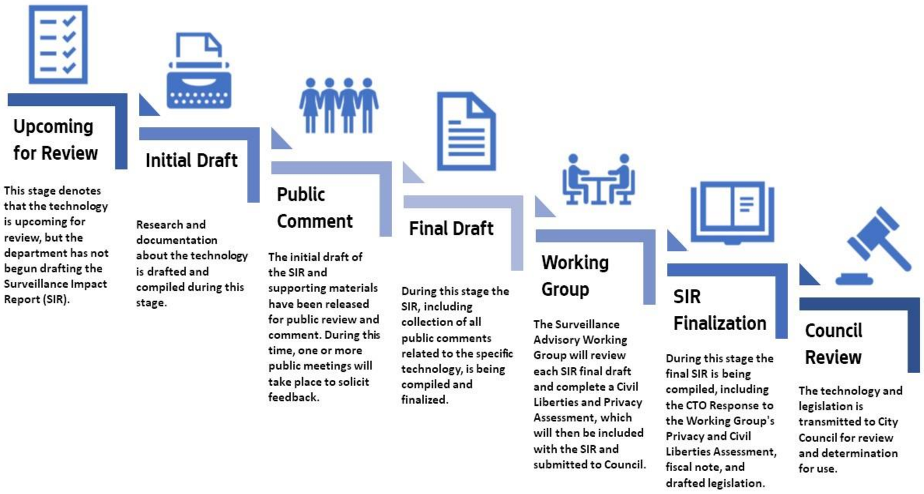
provides information including: (1) a reference list of research and media articles concerning the benefits of the technology; (2) how LPRs relate to SPD's mission; (3) the required training to use the technology; (4) details on when and how often LPRs are in operation; (5) who determines how LPRs are deployed; (5) whether LPRs are visible to the public; (6) a list of the specific outside entities with access to the data; and (7) the experts consulted about the technology.[20]

New York City is the only jurisdiction of those reviewed by OIG-NYPD that does not require community input or legislative decision-making with respect to the selection and use of surveillance technology and the policies and procedures applicable to that technology. The three-person group that reviews the public comments on the draft IUPs consists solely of attorneys employed by NYPD. There is far less robust public oversight of surveillance technologies in New York City than in other locations because (1) NYPD is the sole entity responsible for the collection and review of public comments on the IUPs; (2) the POST Act does not require extensive detail concerning the nature and use of surveillance technology to be included in IUPs (which are public); and (3) there is no legislative or other public body that controls the selection of surveillance technologies, the use of such technologies, and the policies concerning the technologies.

**Figure 2: Seattle Surveillance Technology Review Process**[21]

[20] SEATTLE POLICE DEP'T., 2018 SURVEILLANCE IMPACT REPORT: AUTOMATED LICENSE PLATE RECOGNITION (2019), https://www.seattle.gov/documents/Departments/Tech/Privacy/SPD%20ALPR%20%28Patrol%29%20-%20Final%20SIR.pdf.

[21] Seattle Information Technology, *Surveillance Technologies, Surveillance Impact Report Stages*, http://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies/about-surveillance- (last visited Nov. 1, 2022).



Upcoming for Review

This stage denotes that the technology is upcoming for review, but the department has not begun drafting the Surveillance Impact Report (SIR).

Initial Draft

Research and documentation about the technology is drafted and compiled during this stage.

Public Comment

The initial draft of the SIR and supporting materials have been released for public review and comment. During this time, one or more public meetings will take place to solicit feedback.

Final Draft

During this stage the SIR, including collection of all public comments related to the specific technology, is being compiled and finalized.

Working Group

The Surveillance Advisory Working Group will review each SIR final draft and complete a Civil Liberties and Privacy Assessment, which will then be included with the SIR and submitted to Council.

SIR Finalization

During this stage the final SIR is being compiled, including the CTO Response to the Working Group's Privacy and Civil Liberties Assessment, fiscal note, and drafted legislation.

Council Review

The technology and legislation is transmitted to City Council for review and determination for use.

Furthermore, the POST Act does not require the same type of public comment process that is required by the New York City Administrative Procedure Act ("CAPA").[22] CAPA describes the general process for rulemaking by New York City agencies. Before adopting any rule under CAPA, the agency must not only afford the opportunity for public comment, but advertise that opportunity in specified ways. The comments received are placed into the public record.[23] Agencies must also permit and consider petitions by members of the public to adopt rules that the public proposes.[24] By contrast, the POST Act merely requires that the Department must receive and consider public comments, but does not require that those comments be posted, and does not provide a process for the public to propose, and the Department to consider, particular surveillance technology policies.

### 2. Drafters of the POST Act

In interviews with community organizations and advocacy groups that assisted in the drafting of the POST Act, the Office heard concerns about the manner in which NYPD complied with the legislation. These interviews, which took place after the Department's publication of its draft IUPs, highlighted the following perceived deficiencies of the final IUPs: information about how the tools were deployed was not included; an assessment of the disparate impact of the use of the technology was not included; information on who has access to the data collected was not included; and,

[22] *See generally* N.Y.C. CHARTER §§ 1041-1047.
[23] N.Y.C. CHARTER § 1043(e).
[24] N.Y.C. CHARTER § 1043(g).

detail about which vendors were used was not included. Disclosure of these details, according to the groups and organizations, would be more consistent with their expectations with respect to the POST Act.

### 3. Statutory Minimums vs. Best Practices

The POST Act imposes certain requirements on NYPD with respect to surveillance technologies, but it does not prohibit the Department from providing additional information in the interests of transparency and good governance. Beyond OIG-NYPD's specific responsibilities with respect to auditing NYPD's compliance with the POST Act, its mandate is to "study, audit and make recommendations relating to the operations, policies, programs and practices" of NYPD in order to increase public safety, protect civil rights and civil liberties, and to increase the public's confidence in the police force; thus building stronger police-community relations.[25] OIG-NYPD's position is that NYPD can and should provide additional information about these technologies, where doing so does not compromise the confidentiality of sensitive law enforcement information. The POST Act's requirements establish the minimum with respect to disclosures. But in light of the expectations of community organizations and advocacy groups, the practices in other jurisdictions, and the notice and comment procedure of CAPA, OIG-NYPD recommends improvement to the IUPs, consistent with the requirements of similar legislation around the country and the expectations of those involved in the drafting of the legislation. The Office is sensitive to the need to balance law enforcement confidentiality and public transparency, and the recommendations in this Report offer concrete proposals with this balance in mind.

## IV. Methodology

OIG-NYPD reviewed all 36 draft and final IUPs, examined the POST Act legislation and its history, interviewed a range of individuals including officials from NYPD's Legal Bureau, searched for any complaints received by the Department of Investigation (DOI) alleging that NYPD violated the IUPs, reviewed comparable legislation from other jurisdictions across the country, and conducted a section-by-

[25] N.Y.C. CHARTER § 803(c)(1).

section assessment of one IUP, and an in-depth assessment of two selected technologies and related IUPs.[26]

Interviews with legal experts, advocacy groups (including those who supported and participated in the drafting of the POST Act), community organizations, and subject matter specialists, were central to the data-gathering process. These interviews, as well as a review of City Council hearing testimony concerning the development of the legislation, provided background on the Act.

In its discussions with the Department, OIG-NYPD gathered details related to the processes of drafting IUPs, considering public comments, and finalizing the policies. These discussions informed the Office's understanding of NYPD's process with respect to the POST Act's requirements, and clarified various points related to the content of the IUPs.

As required by the POST Act, OIG-NYPD conducted a review of complaints (from individuals and entities) received by DOI in the 2021 calendar year to identify any potential allegations of violations of the POST Act or IUPs; none of the complaints alleged violations of the IUPs.[27]

To inform any recommendations regarding revisions of the IUPs, OIG-NYPD conducted an in-depth comparative analysis of legislation similar to the POST Act in other relevant jurisdictions. This review was limited to surveillance technology oversight laws in effect for Santa Clara County, California; Seattle, Washington; and San Francisco, California.[28] These jurisdictions were selected due to certain similarities with New York City as to population, urban density, and security threats.

[26] OIG-NYPD received one document, from the Legal Aid Society, presenting arguments that NYPD had violated the POST Act, not any specific IUP. While this complaint does not fall squarely into the Office's responsibility to review and "describe any known or suspected violations of surveillance technology [IUPs]," it was considered for background on public concerns.

[27] Consistent with DOI's policies and practices, OIG-NYPD reviews all complaints received from members of the public or other entities and generally investigates those complaints that raise systemic issues. OIG-NYPD also refers complaints to other agencies (and/or squads at DOI) where the complaints fall within their areas of focus.

[28] While Santa Clara has a smaller population than the other cities, it was selected in part because it was the first city to introduce surveillance technology legislation in the United States (Selena Larson, *Communities Call for More Control Over Police Surveillance*, CNN (Feb. 7, 2017), https://money.cnn.com/2017/02/07/technology/cop-surveillance-aclu-santa-clara-bart/.

OIG-NYPD conducted a section-by-section assessment of the IUP for LPRs. OIG-NYPD assessed each section to evaluate the sufficiency of the information provided (see Appendix C for the full text of the IUP). The language highlighted in blue in Appendix C is included, largely verbatim, in many of the IUPs, and illustrates that much of the content did not clearly identify, among other things, relevant details such as the particular agencies with access to the data gathered via the surveillance technology or the length of time such data would be retained. Following each section of blue highlighted language is a "note box" that indicates the number of IUPs that contain identical or nearly identical statements.

For the in-depth assessments of the IUPs, OIG-NYPD selected FRT and Social Network Analysis Tools. The Office interviewed supervisors from the units responsible for handling the two selected technologies, as well as experts in these technologies. These interviews provided valuable information about NYPD's actual use of the technologies and was supplemented by the Office's review of certified training programs on the use of the surveillance technologies.

## V. Section-by-Section Assessment of LPR IUP

For each section of the IUP for License Plate Readers, OIG-NYPD concluded that the information provided by NYPD largely complied with the requirements of the POST Act, although the IUP could be improved by the inclusion of additional information and clarification about the technology in certain areas, as discussed further below.[29]

1. Capabilities of Technology

The POST Act requires that an IUP include "a description of the capabilities of a surveillance technology." The information provided by NYPD in this section provides an overview of what License Plate Readers are, how the technology works, and the three types of data that are collected. The Department's description of the technology appears both clear and comprehensive, providing information found in other publicly available sources.[30]

2. Rules, Processes, and Guidelines Relating to Use of the Technology

[29] See Appendix C for the full text of the License Plate Readers IUP.

[30] *See, e.g.*, *Automated License Plate Readers*, ACLU OF N.Y., https://www.nyclu.org/en/automatic-license-plate-readers#:~:text=What%20are%20automatic%20license%20plate,its%20date%2C%20time%20and%20location (last visited Nov. 1, 2022).

The POST Act requires that an IUP include "rules, processes[,] and guidelines issued by the [D]epartment regulating access to or use of" the tool, in particular: (1) the rules, processes, and guidelines; (2) any prohibitions or restrictions on its use; and (3) whether court authorization is obtained prior to use. The Office observed that with respect to part (1), the rules, processes, and guidelines governing the use of LPRs, the IUP provides minimal detail. A full list of rules, processes, and guidelines for the use of the data obtained via this technology may exist within relevant Patrol Guide sections, policy memoranda, or Interim Orders, if so, the IUP should link or make clear reference to these materials.

The IUP clearly states the prohibitions and restrictions on use of LPRs, as well as the fact that court authorization is not required to use LPRs, and thus satisfies requirements (2) and (3) noted above.

3. Safeguards and Security Measures Against Unauthorized Access

The POST Act requires the IUP to include the following information with respect to safeguards and security measures against unauthorized access: (1) description of the safeguards or security measures; (2) whether encryption exists; and (3) description of access control mechanisms. The LPR IUP gives sufficient detail about the safeguards and security measures that protect against unauthorized access, notes that the information obtained via LPR is encrypted within NYPD computer systems, and adequately describes the access control mechanisms.

4. Policies and Procedures Relating to Retention, Access, and Use of the Data

The POST Act requires that IUPs include policies and procedures related to (1) the retention of data; (2) access to data; and (3) the use of data. NYPD's IUP provides sufficient information with respect to access to data and lists five circumstances under which use of the data is allowed.

The IUP states that NYPD collects three types of LPR data: (1) a vehicle's license plate number and state of issuance; (2) images of a vehicle and the license plate; and (3) the date, time, and location the vehicle passed the LPR. According to the IUP, these three types of data are retained for five years. The IUP also states that data retention time periods are based on the nature of the "case investigation record," and those periods range from permanent retention of the data to retention for one year. However, the IUP does not make clear under what circumstances LPR data may qualify as a case investigation record or how the 5-year retention period relates to the periods determined based on the nature of the "case investigation records."

### 5. Policies and Procedures Relating to Public Access or Use of the Data

The POST Act requires that the IUP include information regarding policies and procedures related to the public's access to and use of data from surveillance technologies. The LPR IUP makes clear that data obtained from LPRs is available to the public only via a Freedom of Informational Law ("FOIL") request. It would be preferable to include in the IUP a link or reference to the NYPD policy on handling FOIL requests, so that the public could be better informed of the circumstances under which such data could become public.

### 6. External Entities

The POST Act requires IUPs to include the following information concerning third parties' access to surveillance technology data: "whether entities outside the [D]epartment have access to the information and data collected by such surveillance technology, including: (a) whether the entity is a local governmental entity, state governmental entity, federal governmental entity[,] or a private entity, (b) the type of information and data that may be disclosed by such entity, and (c) any safeguards or restrictions imposed by the department on such entity regarding the use or dissemination of the information collected by such surveillance technology[.]"[31] The IUP makes clear that data may be shared with third parties, including government agencies at all levels as well as private vendors and contractors performing contractual duties for NYPD. However, while the IUPs make general references to the types of entities that have access, none of the entities are listed by name.

The IUPs do not make clear whether third parties have access to all three types of LPR data and if not, which third parties have access to which type of data. Furthermore, despite the POST Act's requirement, the IUP does not make clear what, if any, safeguards and restrictions apply to the use of such data by third parties.

### 7. Training

The POST Act requires that IUPs include information regarding whether training is required to use or access information from surveillance tools. The LPR IUP states that users receive "command level training," a vague description that does not give any details about the kind or frequency of training that is required for use or access. Adding this detail would improve the public's understanding of the type of training

[31] POST Act*, supra* note 5.

received by NYPD staff entrusted with access to and use of the data generated by this technology.

8. Internal Audit and Oversight Mechanisms

The POST Act requires a description of any internal audit and oversight mechanisms that ensure compliance with the IUP. The IUP provides general information about who has oversight responsibilities, but gives little detail about the oversight mechanism. Specifically, it is unclear what information is audited by NYPD to monitor compliance with the IUP or how breaches in policy are identified and addressed.

9. Health and Safety Reporting

The POST Act requires information on any tests or reports regarding health and safety impacts of the surveillance tool. The LPR IUP states that there are no "known health and safety issues" with LPRs. In light of the nature of LPRs, this assessment is sufficient for this IUP. However, as noted below, for other technologies, OIG-NYPD recommends that NYPD provide additional information, including, for example, describing efforts made to identify any relevant health and safety tests and reports that may exist and a review of manufacturer warnings or evaluations by experts in the field.

10. Disparate Impacts

The POST Act requires that the IUP include information concerning the "potentially disparate impacts of the surveillance technology [I]mpact and [U]se [P]olicy on any protected groups." In this section, the Department first states that "the safeguards and audit protocols built into this [I]mpact and U]se [P]olicy for LPRs mitigate the risk of impartial [sic] and biased law enforcement." The Department notes that biometric measurements are not collected by LPRs, and then states its policy on impartial enforcement of the law. The IUP does not address the potential disparate impacts of *the use of the technology* and the Act does not require that NYPD provide that information.

Although not required by the POST Act, the Office recommends that NYPD include in the IUP any available information about the potential disparate impacts of the use of the technology. For example, the potential impacts of deploying LPRs in a community are not explored. Important questions about this impact are: Where is this technology typically deployed? Is it deployed more frequently in particular neighborhoods? Does the location and use of technology result in the gathering of more data with respect to members of particular demographic groups, as opposed to other groups? Does NYPD access LPR data obtained from particular neighborhoods more frequently than from other neighborhoods? What are the demographics of the neighborhoods where data is most frequently obtained by NYPD? Does that data more frequently relate to members of particular demographic groups?

## VI. In-Depth Assessment of Selected Technologies

OIG-NYPD conducted in-depth assessments of the Facial Recognition and Social Network Analysis technologies and concluded that the IUPs related to these technologies could be improved by including additional details about: (1) the capabilities of the tools used by NYPD; (2) the extent to which external entities control data captured by the Department's use of these tools; and (3) how NYPD ensures compliance with the IUPs (in particular, what information NYPD reviews to do so).

### A. Facial Recognition Technology

Facial Recognition Technology ("FRT") refers to computer programs that compare facial images to assess their similarity. FRT utilizes a complex series of algorithms and data science to render a photograph of a face into a series of data points — a faceprint — that can then be compared to other faceprints.

Law enforcement agencies typically use FRT for two purposes: (1) to confirm the identity of a suspect, victim, missing person, or to exonerate those who have been wrongfully accused after a crime has occurred; or (2) real-time public surveillance. FRT compares images to a database of known suspects images. Some FRT is capable of facilitating real-time surveillance by comparing known suspect images with images captured by continuously scanning individual's faces (e.g., in a crowd) with a video-capturing device, and responding to those results that reach a threshold of similarity.[32] However, according to NYPD, and as discussed in the FRT IUP, the Department does not have FRT capable of conducting real-time public surveillance. Examples of NYPD's use of this technology to confirm the identity of a suspect after

[32] Any video can be fed through the FRT algorithm, which identifies and isolates faces for comparison.

a crime has occurred include an attempted rape case in August 2020 and an investigation involving suspected bomb containers in the subway in August 2019.[33]

### 1. Public Concerns

Public concern around the use of FRT centers on the risk that its use leads to increased bias in policing, and can curtail the exercise of public speech. There have been allegations that this technology results in disproportionate misidentification of individuals within certain demographic groups.[34] This perception may in part be due to the fact that FRT algorithms most accurately identify members of demographic groups whose photos have been used to "train" the algorithm. For example, studies show that FRT algorithms have higher false positive rates for Asian and Black individuals than for white individuals.[35] An algorithm's inability to distinguish between faces of a particular demographic group can result in increased numbers of mistaken "matches" when used with respect to that group (i.e., false positives).[36] Similarly, the make-up of the database used to search for a possible-match candidate can affect the likelihood of a match. For example, if a database is comprised mostly of men, but the possible-match candidate is a woman, the likelihood of a mistaken identity is increased.

In the wake of various protests in the United States, there have been claims, including by the media, that after protests, police officers outside of New York City were using FRT in order to find and arrest activists, in particular those with outstanding warrants.[37] In one example, Pennsylvania State Police, aided by FRT,

[33] Frank Miles, *NYPD Uses Facial Recognition to Arrest Brazen Sex Offender Accused of Attempted Rape on Subway Platform*, FOX NEWS (Aug. 30, 2020), https://www.foxnews.com/us/nypd-uses-facial-recognition-to-arrest-brazen-sex-offender-accused-of-attempted-rape-on-subway-platform; Craig McCarthy, *How NYPD's Facial Recognition Software ID'ed Subway Rice Cooker Kook*, THE N.Y. POST (Aug. 25, 2019), https://nypost.com/2019/08/25/how-nypds-facial-recognition-software-ided-subway-rice-cooker-kook/.

[34] Davide Castelvecchi, *Is Facial Recognition Too Biased to Be Let Loose?*, NATURE (NOV. 18, 2020), https://www.nature.com/articles/d41586-020-03186-4.

[35] Jan Lunter, *Beating the Bias In Facial Recognition Technology*, BIOMETRIC TECH. TODAY, Oct. 2020, at 5, 5–7, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7575263/.

[36] *See generally* PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, NAT'L INST. OF STANDARDS AND TECH, FACE RECOGNITION VENDOR TEST (FRVT), PART 3: DEMOGRAPHIC EFFECTS (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[37] See, *e.g.*, Kevin Rector & Alison Knezevich, *Social Media Companies Rescind Access to Geofeedia, Which Fed Information to Police During 2015 Unrest*, THE BALTIMORE SUN (Oct. 11, 2016), https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html;

used social media posts to identify individual protesters from details as small as a cross tattoo in the corner of an eye.[38] Advocates warn that such use can discourage people from engaging in protected public speech.[39]

### 2. Assessment of NYPD's Facial Recognition Technology IUP

As required by the POST Act legislation, NYPD published an IUP on its use of FRT. Similar to other IUPs, the policy for FRT largely complies with the Act's requirements, but provides minimal information about NYPD's uses of this surveillance technology, its data sharing and retention practices, oversight of the handling of data generated by this technology, and the potential disparate impacts of its applications.

NYPD informed OIG-NYPD that its staff access FRT through a portal provided by the United States Office of National Drug Control Policy ("ONDCP") New York/New Jersey High Intensity Drug Trafficking Areas ("HIDTA") program. This portal, which uses the DataWorks Face Plus program, compares arrest images, from arrests made in New York or New Jersey, to an image provided by the Department (referred to herein as a "probe" image).[40] The Department informed OIG-NYPD that the DataWorks Face Plus program does not make comparisons to images from drivers licenses or other forms of official identification documents but only to arrest images. As stated in the IUP, NYPD maintains records of all requests, including the original probe image(s) submitted to the Facial Identification Section ("FIS"), which is the unit within the Department charged with FRT administration. Additionally, NYPD

Juliette Rihl, *Emails Show Pittsburgh Police Officers Accessed Clearview Facial Recognition After BLM Protests*, PUBLICSOURCE, (May 20, 2021), https://www.publicsource.org/pittsburgh-police-facial-recognition-blm-protests-clearview/.

[38] Katie Shepherd, *An Artist Stopped Posting Protest Photos Online to Shield Activists from Police. Then, He Was Arrested*, THE WASH. POST (Aug. 3, 2020), https://www.washingtonpost.com/nation/2020/08/03/philadelphia-arrest-protest-photos/

[39] *Street-Level Surveillance, Face Recognition*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/face-recognition#:~:text=Face%20recognition%20is%20a%20method,identify%20people%20during%20police%20stops (last updated Oct. 24, 2017).

[40] Details regarding the DataWorks Plus programs may be referenced on the company's website at www.dataworksplus.com. For information on the FACE Plus program, see *Face Plus, Facial Recognition Technology & Case Management*, DATAWORKSPLUS, https://www.dataworksplus.com/bioid.html#face (last visited Nov. 1, 2022). DataWorksPlus does not create FRT algorithms itself. Instead, it uses algorithms supplied by NEC, Rank One Computing, and Cognitec (Dave Gershgorn, *California Police are Sharing Facial Recognition Databases to ID Suspects*, MEDIUM [Aug. 1, 2019], https://onezero.medium.com/california-police-are-sharing-facial-recognition-databases-to-id-suspects-3317726d31ad; *see also* Grother et al., *supra* note 36).

maintains records of output from the FIS (e.g., possible match candidates). As discussed further below, it is a standard practice in certain circumstances to alter an original probe image to facilitate a search; NYPD also maintains copies of any altered images used for the FRT search. NYPD does not keep records of the results of the searches conducted, and related acts of the FIS staff relating to the search. These acts could include modifying a probe image, which NYPD reported can be done on NYPD computers before uploading the image or it can be done through the DataWorks Face Plus program software accessed through HIDTA.

The way in which NYPD accesses FRT (via a portal provided by HIDTA) has significant implications for NYPD's data retention, data sharing, and auditing practices because many of the details related to the parameters of FRT searches conducted by NYPD are held by HIDTA, the portal owner. In other words, NYPD keeps records of the requests to the FIS unit (i.e., a request to determine whether a probe image matches a known individual in the available databases), the original probe image and any altered images run through the databases, and the output *from* the FIS unit, such as the report to the field investigator of possible matches. However, many other records are controlled by and would need to be requested from HIDTA. Such records would reflect the particulars of each round of searches conducted, including the likelihood that the probe image and the possible match candidates depict the same individual, as well as the details with respect to precisely how altered probe images were modified.

NYPD informed OIG-NYPD that it is capable of auditing FRT searches. However, OIG-NYPD maintains that the need to request search history records from a third-party entity (e.g., the DataWorks Face Plus program run through HIDTA) introduces additional barriers to NYPD and OIG-NYPD's ability to regularly review searches for misuse or policy violations (e.g., searches unrelated to an investigation). How long these records are kept, in what format, and with whom the records could be shared are all controlled by HIDTA. Moreover, NYPD does not have a policy in place to review these past FRT searches and it may have difficulty doing so, because it does not control the database and all of the records that would be subject to review. NYPD also has no policy or process in place to audit how the DataWorks Face Plus program handles the data. NYPD informed OIG-NYPD that its agreement with DataWorks had no terms and conditions in relation to its Face Plus program accessed through HIDTA, including with respect to how data is retained, stored, and protected from disclosure. These terms and conditions would set forth the data retention standards necessary to craft policies around and conduct such an audit. Agreements with HIDTA setting forth polices around data use and auditing are not without precedent. For example, the partnership between the Northern California Regional Intelligence

Center ("NCRIC") and HIDTA produced a policy on Facial Comparison Analysis, which sets forth, among other things, data retention standards, data dissemination standards, and that designated managers and supervisors should conduct periodic audits regarding access to HIDTA's data.[41] NYPD should have a similar policy in place regarding periodic audits of the FIS unit's use of the DataWorks Face Plus program accessed through HIDTA. OIG-NYPD will continue to monitor whether NYPD has sufficient audit-related policies established for other technologies.

NYPD also informed OIG-NYPD that FIS has a process in place (although it is not memorialized in a written policy) for conducting face comparisons. That process includes both the use of the FRT software as well as human reviewers and some internal oversight. In the first step of this process, an investigator in the FIS reviews the quality of the images to be used as probe images. If these images are of poor quality, the risk of misidentification increases. Thus, consistent with industry standards, NYPD FIS investigators have the authority to reject the image and refuse to conduct an FRT software comparison or to modify the image in limited ways in order to improve the quality of the image.[42] NYPD reported to OIG-NYPD that the modifications to the probe images can be made by NYPD prior to uploading the image to the HIDTA portal or within the HIDTA portal after upload, or both.

Modifying probe images to facilitate FRT searches is a common and appropriate manner of using the technology, but model practices emphasize the need to maintain records of any modifications made.[43] For example, model practices include a specified order of modifications, the first step of which is that the probe image can be cropped, resized and/or rotated, the background blurred, and the posing of the face corrected. Those initial changes should be made, and the altered probe image run through the FRT software before the subject's face is modified in any way. The next modification phase of the model practice for an FRT search involves image processing (typically using Adobe Photoshop or GNU Image Manipulation Program [GIMP]) including, but

[41] *Facial Comparison Analysis Policy*, HIDTA/NCRIC (Oct. 2021), https://ncric.ca.gov/wp-content/uploads/2021/10/NCRIC-Facial-Comparison-Analysis-Policy.pdf.

[42] For an example of New York State's model policy on FRT, see N.Y. STATE MUN. POLICE TRAINING COUNCIL, FACIAL RECOGNITION MODEL POLICY (Dec. 2019), https://www.criminaljustice.ny.gov/crimnet/ojsa/standards/MPTC%20Model%20Policy-Facial%20Recognition%20December%202019.pdf.

[43] *See* FACIAL IDENTIFICATION SCI. WORKING GRP., STANDARD PRACTICE/GUIDE FOR IMAGE PROCESSING TO IMPROVE AUTOMATED FACIAL RECOGNITION SEARCH PERFORMANCE (July 17, 2020). https://fiswg.org/fiswg_image_proc_to_improve_fr_search_v2.0_2020.07.17.pdf.

not limited to, color/tint correction, de-blurring or sharpening, lens distortion correction, red eye reduction, and other modifications. The altered probe images resulting from these modifications should be run through the FRT software at specific points in that process and may produce a different candidate search result set. Finally, the subject's face can be modified including, but not limited to, changes to hair, head coverings, replacing or creating missing facial landmarks, and altering excessive make-up, which may produce yet another candidate set. According to the model practices, after certain points in the progression of image processing, an FRT search should take place and the match candidates evaluated.[44]

In contrast with the stringent model practices set forth above, NYPD did not report using *any* guidelines to specify the types, order, or number of modifications that could be conducted, and at what points in the alteration process searches should be run. Also, in contrast with the model practices, NYPD edits probe images using Microsoft Paint, a basic graphics editor, among other programs. Although NYPD also uses Adobe Photoshop to make modifications, which is in accordance with model practices, notably NYPD does not utilize Adobe Photoshop's Edit History log and stated that it was unaware of how much detail the Edit History log contains with respect to modifications. Adobe Photoshop allows users to turn on and off the Edit History log and to choose what level of modification detail is retained. However, NYPD does not have a policy requiring the Edit History log to be turned on. Therefore, it is unclear which, if any, of NYPD's edits in Adobe Photoshop have been retained and can be reviewed.

Moreover, although NYPD retains records of rejections by the FIS due to low quality, as well as the altered probe images run through the FRT software, it does not retain logs of each individual modification made to produce the altered probe images, whether modifications occurred on NYPD computers or through the HIDTA portal nor does NYPD retain notes about the points in time during the modification process that searches were conducted. The failure to track individual modifications that are made to the probe images limits potential oversight of how images are altered in the course of a search – failure to alter images in the appropriate manner can result in misidentification. However, this concern could be readily avoided if NYPD used the model practice of (1) making the process of face comparison iterative and (2)

[44] *Id.*

documenting modifications to the images.[45] NYPD should put policies and procedures in place delineating the process by which FIS investigators should modify a probe image in a specified manner and order and run the modified image through the FRT software, review the FRT software output, modify the probe image again, conduct the FRT comparison again, and retain the search results with respect to each altered probe image used to search. If the Department tracked modifications to probe images, it would have a record that could be used to determine whether the FIS modified images pursuant to stated policy (and the industry standard) or in a way that might raise the risk of misidentification. Without an accurate log of these modifications, the record of exactly which modifications created the altered images is lost, foreclosing review by NYPD or OIG-NYPD.

NYPD *did* provide information about the potential disparate impact of the use of FRT itself (as opposed to the disparate impact of the IUP) in the FRT IUP. As noted above, however, NYPD did not provide this information in 31 out of 36 IUPs, opting instead to address the potential disparate impact of the IUPs themselves. In the FRT IUP, the Department acknowledged research highlighting poor performance by some algorithms in matching photographs of individuals from certain racial and/or ethnic groups, if the algorithms were not trained with respect to those groups.[46] The IUP also noted "an important federal government study on the subject" that suggested that human review of FRT matches could alleviate such errors. This study, however, is not cited in the IUP. When asked for the study in connection with the preparation of this Report, NYPD claimed that a National Institute of Standards and Technology study presents evidence that "erroneous software matches can be swiftly corrected by human observers." OIG-NYPD reviewed that study and concluded that it does not support NYPD's claim that human observation can remedy erroneous software matches. In fact, to the contrary, the study does not address human observation

[45] For example, the NCRIC and HIDTA policy on Facial Comparison Analysis sets forth that any enhancements to a probe image should be made on a copy, saved separately, and documented to show what enhancements were made, including the date and time of the change and the results of the search (*Facial Comparison Analysis Policy*, HIDTA/NCRIC [Oct. 2021], https://ncric.ca.gov/wp-content/uploads/2021/10/NCRIC-Facial-Comparison-Analysis-Policy.pdf.)

[46] Brendan F. Klare et al., *Facial Recognition Performance: Role of Demographic Information*, 7 IEEE TRANSACTIONS ON INFO. FORENSICS AND SEC. 1789 (2012), https://s3.documentcloud.org/documents/2850196/Face-Recognition-Performance-Role-of-Demographic.pdf.

except to state that "the interaction of machine and human is beyond the scope of this [study], as is human efficacy."[47]

### B. Social Network Analysis Tools

While the applicable IUP refers to "social network analysis tools," NYPD's use of such tools, which create network maps illustrating social relationships, is limited. In fact, NYPD uses social *media* analysis technology. This technology searches social media platform (e.g., Facebook, Instagram) content using artificial intelligence, allowing law enforcement to track and monitor publicly available social media content for information relevant to investigations and potential threats.[48]

#### 1. Public Concerns

Public concerns about the use of social media analysis technology centers around the constitutional right to privacy and the ethical implications of law enforcement's use of fake social media accounts. For example, the Brennan Center claims that law enforcement tracking of individuals and political events through social media is an invasion of privacy and violates the public's First Amendment right to free speech. Similarly, the Brennan Center claims that such tracking violates an individual's First Amendment freedom to assemble and protest.[49]

Advocacy groups also expressed concern about law enforcement's use of fake social media accounts to gain access to individuals' posted information and social networks. These groups noted that police used inappropriate lures such as photos of young women to gain access, and pointed out that, once a person 'friends' or 'follows' NYPD's

[47] Grother et al., *supra* note 36 at 5.
In response to OIG-NYPD, the Department cited the above National Institute of Standards and Technology (NIST) study as stating that, "the application of facial recognition algorithms can be used as part of a hybrid machine-human system," and that, "the full consideration of systems comprised of automated face search algorithms and human reviewers remains an issue for further academic and operational attention." As noted above, the study references hybrid machine-human systems, but notes that assessing a human reviewer's accuracy and efficiency is "beyond the scope" of the study.
[48] *See generally* JOHN S. HOLLYWOOD, ET AL., THE RAND CORP., USING SOCIAL MEDIA AND SOCIAL NETWORK ANALYSIS IN LAW ENFORCEMENT (2018), https://www.rand.org/content/dam/rand/pubs/research_reports/RR2300/RR2301/RAND_RR2301.pdf.
[49] *Statement of Civil Rights Concerns About Monitoring of Social Media by Law Enforcement,* BRENNAN CTR. FOR JUSTICE (Nov. 6, 2019), https://www.brennancenter.org/our-work/research-reports/statement-civil-rights-concerns-about-monitoring-social-media-law.

fake account, the Department may then scan that individual's connections to create lists of affiliations (e.g., to determine whether that individual has potential gang affiliations).[50]

### 2. Assessment of NYPD's Social Network Analysis Tools IUP

NYPD's IUP concerning "social network analysis tools" presents minimal detail about the capabilities, use, data sharing, and oversight with respect to these types of surveillance technologies. Although not included in the IUP, OIG-NYPD's investigation discovered that the Department uses a specific social media analysis tool to support its investigations and intelligence-gathering functions.[51] For example, in the course of an investigation, NYPD officers may obtain a first name or social media handle for a suspect, and then use the tool to conduct a sweep of major social media platforms for likely matches with that individual suspect in an effort to identify them.

The IUP states that "information accessible to NYPD personnel using social network analysis technology is limited to publicly available information, or information that is viewable as a result of user privacy settings or practices."[52] While this statement is accurate, OIG-NYPD found that the Department also seeks and obtains access to information otherwise shielded by privacy settings by creating fake accounts to which targets of surveillance grant access. Moreover, the Department has publicly disclosed its use of fake accounts in investigations and indicated that guidelines exist around their use.[53] The Office's review found that although these guidelines provide a process

[50] *See* Miranda Murillo, Leah Rosenberg & Michael Rebuck, *Undercover Policing in the Age of Social Media,* POLICING PROJECT, NYU SCHOOL OF LAW (December 17, 2018), https://www.policingproject.org/news-main/undercover-policing-social-media;
Joseph Goldstein & J. David Goodman, *Frisking Tactic Yields to a Focus on Youth Gangs*, N.Y. TIMES (Sept. 18, 2013), https://www.nytimes.com/2013/09/19/nyregion/frisking-tactic-yields-to-a-focus-on-youth-gangs.html?ref=todayspaper&pagewanted=all&_r=0.

[51] At NYPD's request and based on its position that the name of the social media analysis tool is law enforcement sensitive information, this Report does not include the name.

[52] N.Y.C. POLICE DEP'T., SOCIAL NETWORK ANALYSIS TOOLS: IMPACT AND USE POLICY (Apr. 11, 2021) https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/social-network-analysis-tools-nypd-impact-and-use-policy_4.9.21_final.pdf.

[53] Rocco Parascandola, *New York Police Dept. Issues First Rules for Use of Social Media During Investigations*, N. Y. DAILY NEWS (Sept. 11, 2012), https://www.nydailynews.com/new-york/new-york-police-dept-issues-rules-social-media-investigations-article-1.1157122.

for officers to obtain permission to use fake accounts, the guidelines were not specific to *how* the fake account could be used.

The Department does not create or maintain the records necessary to audit or otherwise review the use of the social media analysis tool. The Department does not maintain a history of investigator activity in the program. The Department does not know whether the company, which owns the program, retains such records. As a practical matter this means that NYPD cannot and does not review the social media sweeps that it conducts with the assistance of the company for potential misuse. This third-party ownership of the data greatly limits NYPD and/or OIG-NYPD's ability to audit officers' use of the technology. It also limits the Department's ability to determine whether its officers' search histories and results are shared with other entities/parties.

## VII. Key Findings from Review of All IUPs

The information provided by NYPD in the IUPs largely complies with the requirements of the POST Act legislation. As set out in detail above, the POST Act requires NYPD to publish IUPs that include information relating to ten areas, such as capabilities of the surveillance technologies, rules and guidelines governing their use and access to the collected data. The IUPs largely comply with that requirement because information that relates to these areas is included in each IUP. OIG-NYPD observed, however, that rather than develop policies specific to these surveillance technologies, the IUPs largely restate existing Department policy. With respect to disparate impact, for example, the majority of the IUPs simply refer to NYPD's existing policies concerning the Department's commitment to unbiased enforcement of the law; the IUPs do not explore whether or how a particular surveillance technology might have a disparate impact. In an interview with OIG-NYPD, NYPD specifically stated that, given the way in which the disparate impact section of the POST Act is drafted, NYPD interprets the Act to require disclosure of the potential disparate impact of *the IUP itself* – but not the potential disparate impact of use of the technology (see below sub-section B for examples of these policies).

As noted above, while the IUPs largely comply with the requirements of the POST Act, OIG-NYPD recommends the improvements described herein in order to improve transparency, as well as meaningful public oversight with respect to NYPD's use of surveillance technology, and also to facilitate OIG-NYPD's audit of NYPD's compliance with the IUPs. These improvements would also be consistent with the expectations of those organizations involved in drafting the POST Act, and with the requirements of similar legislation across the country. In particular, these organizations expressed the view that the IUPs were intended to provide detailed information such as the exact surveillance technologies used, to identify any outside agency that has access to data obtained thereby, and to disclose any potential disparate impacts of the use and deployment of the technology.[54]

As illustrated in OIG-NYPD's section-by-section assessment and in-depth assessments, many of the existing IUPs, while largely complying with the POST Act, do not provide more than a generic level of detail with respect to the above-referenced topics and thus limit meaningful public oversight of NYPD's use of surveillance technologies.

### A. NYPD Uses Vague, Non-Specific Boilerplate Language Throughout the IUPs

As previously noted, in many of the sections of the IUPs, NYPD repeatedly used the same boilerplate language to respond to the information requirements of the POST Act. As a reference point, the table in Appendix C illustrates the extent to which NYPD used identical or nearly identical content for many sections of the final 36 IUPs. For example, 83% of the IUPs use essentially the same language in the "Rules, Processes, and Guidelines Relating to Use" section. While boilerplate language may be sufficient to describe rules and processes that are in fact identical, some of the general language at issue here was insufficiently specific and thus failed to provide relevant information to the public. For example, the IUPs use the same language to describe access to information, without addressing circumstances in which a third-party vendor that supplies a particular technology may have access to the data collected by that technology. NYPD also used boilerplate language to address the Health and Safety component of the technologies, despite readily available individualized information for certain technologies, such as the FCC's potentially hazardous electromagnetic interference classification for electronic devices. This sort of general language also fails to provide clear direction to NYPD — for example with respect to what access is permissible on the part of third-party vendors — and hinders OIG-NYPD's ability to conduct meaningful audits of compliance with the IUPs.

[54] *See Coalition of Advocates and Academics Submit Joint Comments Documenting the NYPD's Failure to Comply with the POST Act*, BRENNAN CTR. FOR JUSTICE (Feb. 24, 2021), https://www.brennancenter.org/our-work/research-reports/coalition-advocates-and-academics-submit-joint-comments-documenting-nypds.

### 1. External Entities' Access to Data

For all categories of surveillance technologies, the IUP sections titled "External Entities," include the same boilerplate language and very little additional information. The POST Act requires information concerning, "whether entities outside the [D]epartment have access to the information and data collected by such surveillance technology, including: (1) whether the entity is a local governmental entity, state governmental entity, federal governmental entity or a private entity, (2) the type of information and data that may be disclosed by such entity, and (3) any safeguards or restrictions imposed by the [D]epartment on such entity regarding the use or dissemination of the information collected by such surveillance technology."[55]

The IUPs for all categories of surveillance technologies address the first requirement by stating: "Government agencies at the local, state, and federal level, including law enforcement agencies other than NYPD, have limited access to NYPD computer and case management systems. Such access is granted by NYPD on a case-by-case basis subject to the terms of written agreements between NYPD and the agency receiving access to a specified system." While this policy statement largely complies with the POST Act by addressing the types of entities with access to surveillance technology data, it is so broad and general that it fails to convey to the public any specific information about the agencies that can access the relevant data. The public would benefit from additional transparency with respect to those agencies that can be granted access to the data, at an appropriate level of generality so as to protect law enforcement sensitive or confidential information. Furthermore, NYPD does not meet the POST Act's second requirement because the IUPs generally do not specify the type of information and data that may be disclosed by such entity. NYPD should begin complying with the provision of the POST Act by providing such information going forward.

Moreover, NYPD includes boilerplate language in numerous IUPs that states "[t]he terms of the written agreements also charge these external entities with maintaining the security and confidentiality of information obtained from NYPD, limiting disclosure of that information without NYPD approval." However, NYPD does not satisfy the third requirement with this language because the IUP does not set forth the particular safeguards and restrictions imposed on each entity with respect to the information to which that entity has access.

[55] POST Act*, supra* note 5.

Additionally, the third-party ownership of some of NYPD's surveillance technologies (e.g., FRT, social media analysis tools) presents challenges to the maintenance of NYPD safeguards and restrictions on the use or dissemination of data, as well as to transparency and oversight with respect to what entities can access data. In light of third-party ownership, it is possible that data generated by certain technologies may be owned, shared, and sold by the third-party owners of the technology, overriding NYPD's control of data sharing and access. A vendor's right of access and disclosure of the data is generally included within the agreements between NYPD and the vendors that supply the technology, and may be limited by such agreements. But, to take just one example, the Department was unable to produce the third-party vendor's Terms of Use agreement for its social network analysis tools provider because it had arranged the purchase through the New York Department of Information Technology & Telecommunications ("DoITT"). Furthermore, the Department was unable to supply the terms and conditions or other information concerning these vendor's access. Without this agreement (or the terms of the agreement) in hand, it is unclear to OIG-NYPD how the Department could comprehensively report on data access by external entities in the IUP.

### 2. Health and Safety Reporting

The Act directs NYPD to provide information in the IUPs concerning, "any tests or reports regarding the health and safety effects of the surveillance technology." The IUPs use boilerplate language to address this issue, stating, in 33 of 36 IUPs (92%), that "there are no known health and safety issues with [technology name] or associated equipment." OIG-NYPD asked what efforts, if any, the Department made to learn about health and safety issues related to its surveillance technologies; NYPD responded that the Department did not conduct any new research. Although NYPD stated that it was not aware of any health and safety issues, it also made no effort to determine whether any tests or reports existed concerning the health and safety effects of specific surveillance technologies, nor did it review any such tests or reports in connection with the preparation of the IUPs. It is also unclear what efforts the Department previously made in this regard.

### 3. Retention, Access, and Use of the Data

For the IUP section on "Policies and Procedures Relating to Retention, Access & Use of the Data," NYPD is required to provide information about how data is held and used. NYPD's boilerplate response in this section begins by describing two sources of regulations concerning records retention generally: The Retention and Disposition

Schedule for New York Local Government Records; and the NYC Department of Records and Information Services supplemental records retention and disposition schedule.

NYPD's IUPs do not consistently explain which record retention policy applies for each technology. For example, NYPD's IUP for LPRs states "[d]ata collected through NYPD's LPRs is retained for five (5) years." But the IUP also references a scale of different retention periods applicable to "case investigation records;" the retention period depends on the nature of the investigation at issue. Within this section of the IUP, the Department lists 15 different types of offenses along with the record retention period. For example, case investigation records classified as a violation or traffic infraction must only be retained for one year after the case is closed. The IUP does not explain whether the five-year retention period applies or whether (and when) LPR data is subject to the case investigation retention period. At a minimum, the IUP should explain the method by which surveillance technology data is categorized for purposes of applying these record retention policies – for example, how is it determined whether the data gathered through use of a surveillance technology qualifies as a "case investigation record" of a particular offense type.

### B. NYPD Has Interpreted the Requirement to Include Information About Potentially Disparate Impacts in a Narrow Manner

The POST Act requires NYPD to provide information regarding, "any potentially disparate impacts of the surveillance technology [I]mpact and [U]se [P]olicy on any protected groups as defined in the New York City [H]uman [R]ights [L]aw." In response, for all IUPs, the Department begins the disparate impacts section with: "The safeguards and audit protocols built into this [I]mpact and [U]se [P]olicy for [insert surveillance technology name] mitigate the risk of impartial [sic] and biased law enforcement." Additionally, in 31 of the 36 IUPs, the disparate impact section offers the above statement and little more than boilerplate language about NYPD's commitment to impartial enforcement of the law, while only five IUPs present the potential disparate impacts of the use of the technology.

The Department explained that it interpreted the Act, and in particular the reference to "disparate impacts of the surveillance technology [I]mpact and [U]se [P]olicy," to require disclosure of the potential disparate impact of *the IUP itself* – not the potential disparate impact of use of the technology.[56] While the language in the IUPs

[56] NYPD is prohibited by law from writing a policy (including IUPs) that would be biased against legally protected groups.

may largely comply with the POST Act's requirement, OIG-NYPD recommends that NYPD provide information about the potential disparate impact arising from the *use of the technology*, in the interests of transparency and so that NYPD can assure the public that any potential disparate impacts are being considered and addressed.

### C. NYPD Has Grouped Related Tools Together in a Way That Limits Public Oversight

While NYPD claims that there are published IUPs applicable to all surveillance technologies as defined by the POST Act, NYPD stated that certain published IUPs cover groups of similar technologies, as opposed to individual technologies. That is, because of the similarity and overlap of some surveillance technologies, NYPD claimed that it was appropriate to group the technologies under a single IUP that described their general capabilities and use (e.g., Data Analysis Tools, Audiovisual Recording Devices, Situational Awareness Cameras). According to NYPD, grouping similar technologies together was also more efficient and facilitated its ability to meet the mandated 180-day deadline. The Department also stated that grouping similar technologies improved the effectiveness of the IUPs by limiting the number of repetitive policies that needed to be memorized by operational NYPD staff.

This approach poses a risk that groupings of technologies could shield individual technologies from public scrutiny and oversight. For example, there is no individual IUP for Digidog, a robot in the form of a dog with mounted microphones and cameras, which NYPD piloted in live operations on several highly publicized occasions.[57] Digidog was grouped into the IUP for Situational Awareness Cameras. As a result, the unique mobility capabilities, safety concerns, third-party ownership, and potential disparate impacts associated with Digidog, if any, were not disclosed to the public or City Council. Other technologies may be similarly shielded from disclosure by grouping.

[57] Mihir Zaveri, *N.Y.P.D. Robot Dog's Run is Cut Short after Fierce Backlash*, N.Y. TIMES (May 11, 2021), https://www.nytimes.com/2021/04/28/nyregion/nypd-robot-dog-backlash.html.

It is the OIG-NYPD's position that the most logical reading of the POST Act's language is that it requires an IUP for each surveillance technology.[58] Moreover, NYPD's interpretation of the POST Act that permits grouping significantly undermines other requirements of the Act. For example, grouping may enable NYPD to bypass the POST Act's disclosure requirements for new technologies. That is, NYPD's grouping approach could allow NYPD to introduce new technologies under an existing group category covered by an existing IUP, and begin use immediately without the required notification to the public and City Council. This allows NYPD to avoid the public notification process – a critical aspect of the POST Act – and thus cannot have been the intent of the legislation.[59]

Grouping also poses a practical barrier to OIG-NYPD's obligations and duties under the POST Act. When OIG-NYPD discussed this grouping strategy with the Department, NYPD stated that it had compiled an internal itemized list of its surveillance technologies to assemble the groups, and this list could be used to audit compliance with the POST Act. OIG-NYPD reviewed this list but the list did not include information concerning the functionality/capability of each technology — information necessary to assess whether the functionalities of various technologies are in fact the same. Without that level of detail, OIG-NYPD cannot assess whether NYPD has issued an IUP that covers each technology with distinct functionalities/capabilities. Furthermore, the list that OIG-NYPD received itself grouped various surveillance technologies. Therefore, due to the limited information provided by NYPD, it is not possible for OIG-NYPD to assess whether the grouping strategy allows for sufficient compliance with the POST Act, and whether NYPD is, in fact, issuing IUPs with respect to each individual surveillance technology (or functionality). OIG-NYPD recommends NYPD discontinue its practice of grouping.

[58] This reading also is supported by the language of the POST Act. It defines an IUP with reference to "*a* surveillance technolog*y*", the singular form of the noun, not "*the* surveillance technolog*ies*." N.Y.C. Admin. Code § 14-188(a) (emphasis added). Further, the definition of surveillance technology also uses a sentence structure that presumes the singular form of technology "that *is* operated by [NYPD]" as opposed to the plural form of technologies "that *are* operated by [NYPD]." *See id.* (emphasis added).

[59] If the POST Act allowed for grouping in the manner described, then the language in N.Y.C. Admin. Code § 14-188(b) mandating a 90-day waiting period before the use of new technology would appear to be unnecessary. In addition, N.Y.C. Admin. Code § 14-188(d) provides a separate path for addendums, thus the POST Act clearly distinguishes between the enhancement of existing technology and the acquisition of entirely new technology. This distinction suggests that the POST Act was not intended to allow grouping.

To the extent that the POST Act is ambiguous, OIG-NYPD's recommendations would benefit from codification from City Council to provide further clarity.

## VIII. Recommendations

Based on the findings of this Report, OIG-NYPD makes the following recommendations:[60]

1. NYPD should issue an IUP for each individual surveillance technology, as opposed to continuing its practice of grouping similar technologies under a single IUP.

2. NYPD should identify in each IUP each external agency, by name, with which the Department can share surveillance data.

3. NYPD should include in each IUP the specific safeguards/restrictions on use or dissemination of the surveillance data, for each external agency with which the Department can share such data.

4. NYPD should include in each IUP the potential disparate impacts on protected groups of the use and deployment of the surveillance technology itself.

5. NYPD should revise the Health & Safety Reporting sections of all published IUPs, to include any safety hazards that are identifiable on the basis of existing research, manufacturer warnings, or evaluations by experts in the field, or to state that no such hazards have been identified after a search for relevant information.

6. Within 180 days, NYPD should convene a working group of NYPD personnel, relevant City Council members or their appointees, and representatives from select advocacy groups and community organizations who have expertise in surveillance technologies. The purpose of the working group is to make recommendations to NYPD on necessary updates to the existing IUPs and on any information that should be included in any future IUPs for new technologies, based on the group's expertise. NYPD's procedures applicable to the working group should ensure the protection of sensitive information as appropriate.

[60] Note that no recommendation requires NYPD to reveal information classified as sensitive to the public.

7. Within 180 days, NYPD should create an internal tracking system for every instance in which NYPD provides an external agency with data collected via surveillance technologies that NYPD controls, including the name of the agency and the date of that the data was provided.

8. Within 90 days, in order to facilitate OIG-NYPD's statutorily obligated audit under the POST Act, NYPD should provide OIG-NYPD with information indicating, for each surveillance technology, the various types of data collected and which NYPD units maintain that information. NYPD should include information about the retention procedures and practices for each type of data collected so that OIG-NYPD can assess NYPD's compliance with the IUPs.

9. NYPD should provide OIG-NYPD with any data access and retention policies that are included in the existing contracts with vendors who supply the surveillance technologies used by NYPD.

10. NYPD should provide OIG-NYPD with the data access and retention policies contained in any newly executed contracts with surveillance technology vendors by the 15th of each quarter (i.e., January, April, July, and October).

11. Within 30 days, NYPD should provide OIG-NYPD an itemized list of the surveillance technologies that it uses. This list should include information concerning the functionalities of each technology, so that OIG-NYPD can assess whether NYPD has, in fact, issued an IUP that covers each surveillance technology that has a distinct functionality or capability.

12. NYPD should create written policies establishing guidelines to specify the modifications that can be made to probe images used for Facial Recognition Technology.

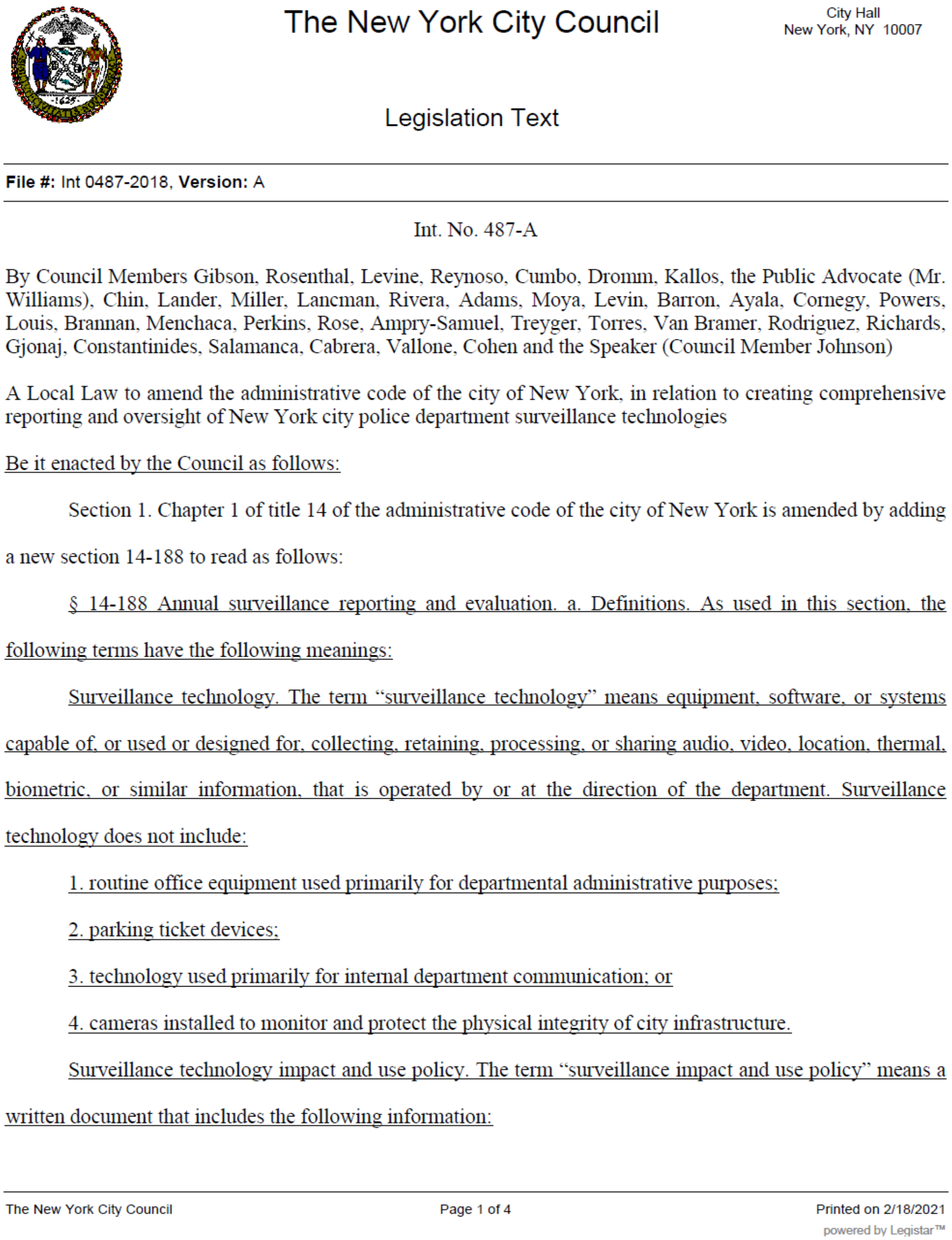
13. NYPD should conduct periodic audits of its Facial Identification Section's use of facial recognition technology to ensure compliance with its policies related to the use of the technology and its data. This auditing process should be memorialized in writing.

14. To facilitate the OIG-NYPD's mandated annual audits, beginning January 15, 2023, NYPD should provide OIG-NYPD with quarterly updates, reflecting newly acquired or discontinued technologies in an itemized list of the surveillance

technologies that it uses. Thereafter, updates should be made available by the 15th of each quarter (i.e., January, April, July, and October).

15. NYPD should issue a press release announcing the publication, related public comment period of any new IUPs, and subsequently publish the press release on its website.

## IX. Appendix A: Text of POST Act Legislation



The New York City Council

City Hall
New York, NY 10007

Legislation Text

**File #:** Int 0487-2018, **Version:** A

Int. No. 487-A

By Council Members Gibson, Rosenthal, Levine, Reynoso, Cumbo, Dromm, Kallos, the Public Advocate (Mr. Williams), Chin, Lander, Miller, Lancman, Rivera, Adams, Moya, Levin, Barron, Ayala, Cornegy, Powers, Louis, Brannan, Menchaca, Perkins, Rose, Ampry-Samuel, Treyger, Torres, Van Bramer, Rodriguez, Richards, Gjonaj, Constantinides, Salamanca, Cabrera, Vallone, Cohen and the Speaker (Council Member Johnson)

A Local Law to amend the administrative code of the city of New York, in relation to creating comprehensive reporting and oversight of New York city police department surveillance technologies

Be it enacted by the Council as follows:

Section 1. Chapter 1 of title 14 of the administrative code of the city of New York is amended by adding a new section 14-188 to read as follows:

§ 14-188 Annual surveillance reporting and evaluation. a. Definitions. As used in this section, the following terms have the following meanings:

Surveillance technology. The term "surveillance technology" means equipment, software, or systems capable of, or used or designed for, collecting, retaining, processing, or sharing audio, video, location, thermal, biometric, or similar information, that is operated by or at the direction of the department. Surveillance technology does not include:

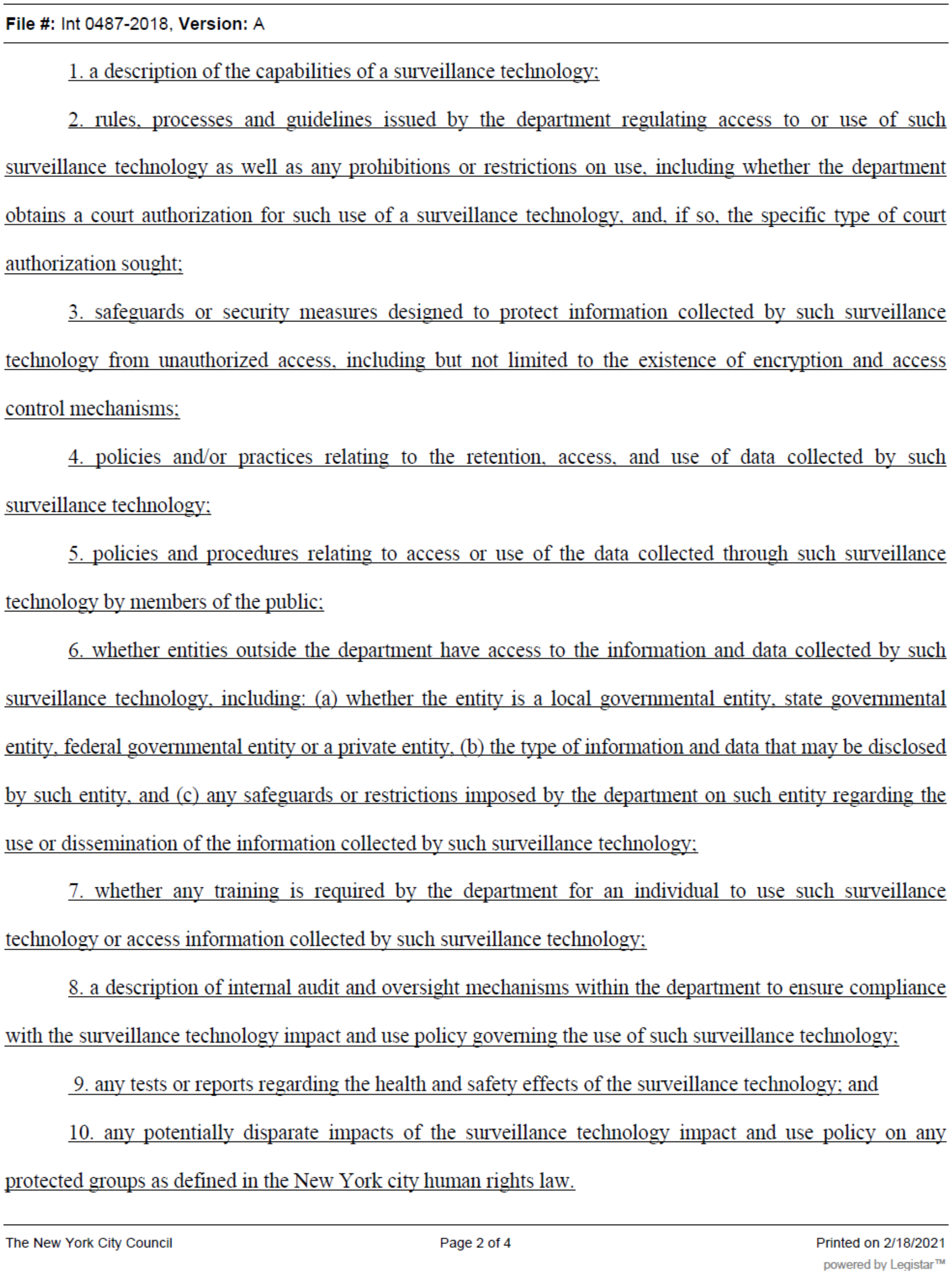
1. routine office equipment used primarily for departmental administrative purposes;

2. parking ticket devices;

3. technology used primarily for internal department communication; or

4. cameras installed to monitor and protect the physical integrity of city infrastructure.

Surveillance technology impact and use policy. The term "surveillance impact and use policy" means a written document that includes the following information:



**File #:** Int 0487-2018, **Version:** A

1. a description of the capabilities of a surveillance technology;

2. rules, processes and guidelines issued by the department regulating access to or use of such surveillance technology as well as any prohibitions or restrictions on use, including whether the department obtains a court authorization for such use of a surveillance technology, and, if so, the specific type of court authorization sought;

3. safeguards or security measures designed to protect information collected by such surveillance technology from unauthorized access, including but not limited to the existence of encryption and access control mechanisms;

4. policies and/or practices relating to the retention, access, and use of data collected by such surveillance technology;

5. policies and procedures relating to access or use of the data collected through such surveillance technology by members of the public;

6. whether entities outside the department have access to the information and data collected by such surveillance technology, including: (a) whether the entity is a local governmental entity, state governmental entity, federal governmental entity or a private entity, (b) the type of information and data that may be disclosed by such entity, and (c) any safeguards or restrictions imposed by the department on such entity regarding the use or dissemination of the information collected by such surveillance technology;

7. whether any training is required by the department for an individual to use such surveillance technology or access information collected by such surveillance technology;

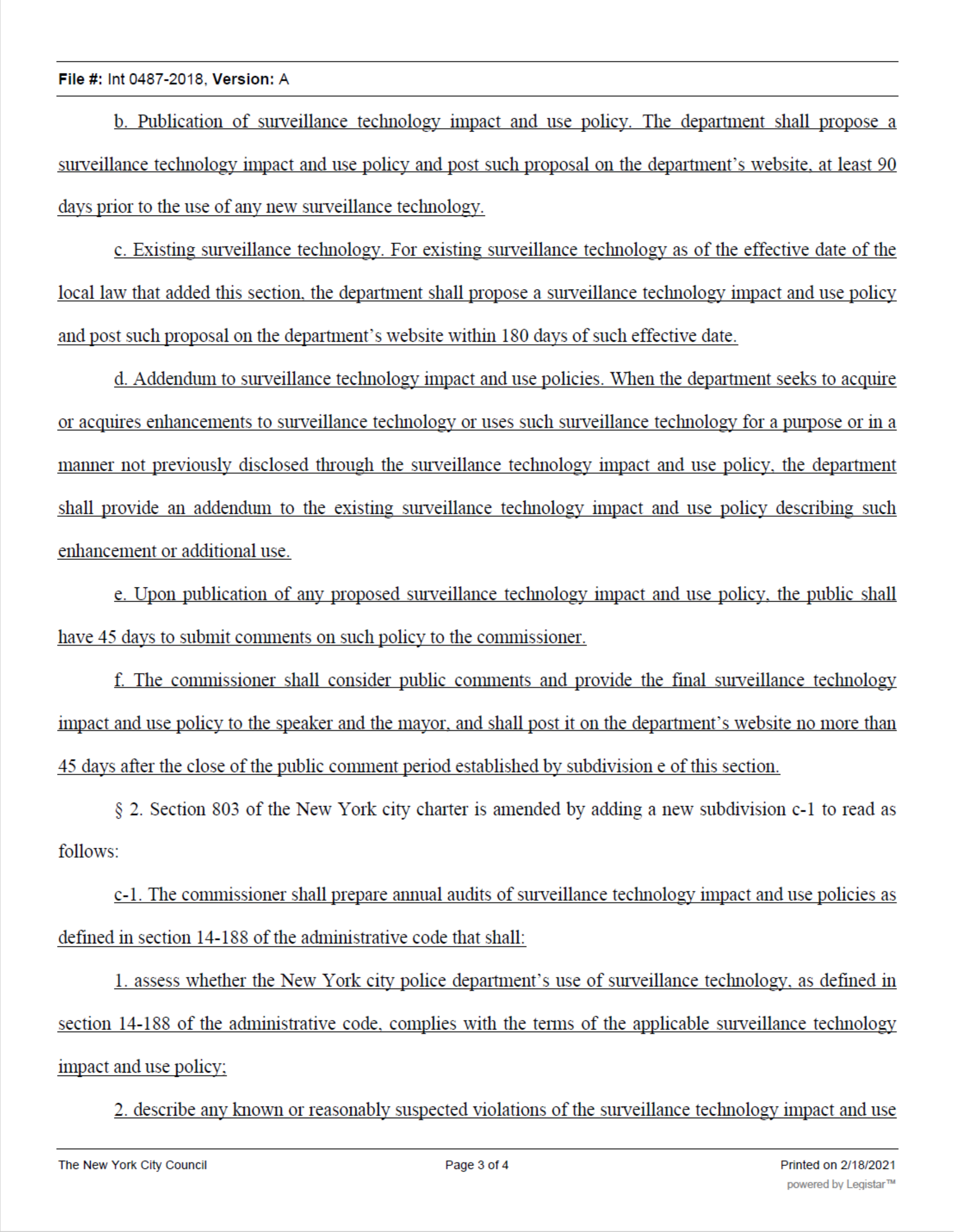
8. a description of internal audit and oversight mechanisms within the department to ensure compliance with the surveillance technology impact and use policy governing the use of such surveillance technology;

9. any tests or reports regarding the health and safety effects of the surveillance technology; and

10. any potentially disparate impacts of the surveillance technology impact and use policy on any protected groups as defined in the New York city human rights law.

The New York City Council Page 2 of 4 Printed on 2/18/2021

powered by Legistar™



**File #:** Int 0487-2018, **Version:** A

b. Publication of surveillance technology impact and use policy. The department shall propose a surveillance technology impact and use policy and post such proposal on the department's website, at least 90 days prior to the use of any new surveillance technology.

c. Existing surveillance technology. For existing surveillance technology as of the effective date of the local law that added this section, the department shall propose a surveillance technology impact and use policy and post such proposal on the department's website within 180 days of such effective date.

d. Addendum to surveillance technology impact and use policies. When the department seeks to acquire or acquires enhancements to surveillance technology or uses such surveillance technology for a purpose or in a manner not previously disclosed through the surveillance technology impact and use policy, the department shall provide an addendum to the existing surveillance technology impact and use policy describing such enhancement or additional use.

e. Upon publication of any proposed surveillance technology impact and use policy, the public shall have 45 days to submit comments on such policy to the commissioner.

f. The commissioner shall consider public comments and provide the final surveillance technology impact and use policy to the speaker and the mayor, and shall post it on the department's website no more than 45 days after the close of the public comment period established by subdivision e of this section.

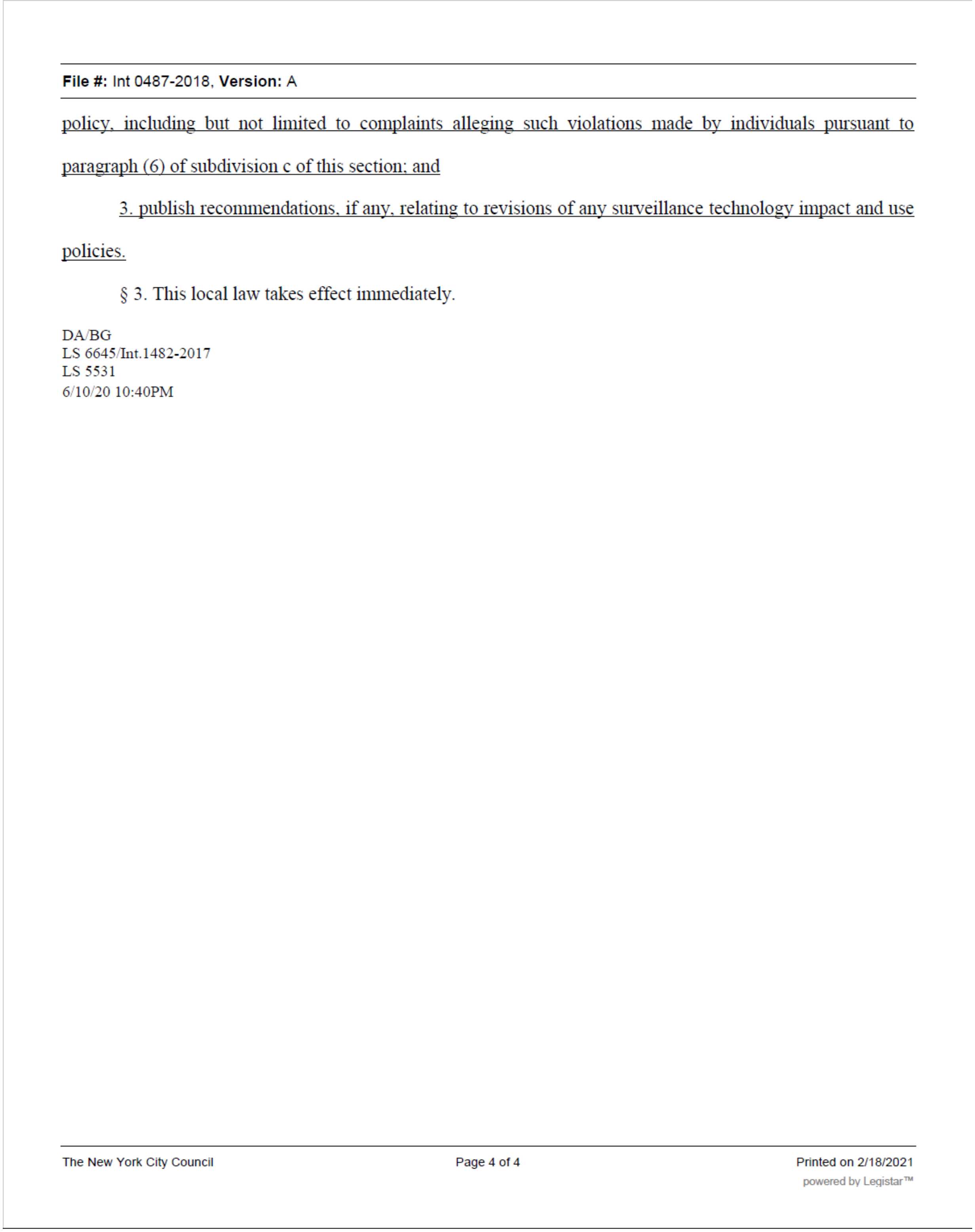
§ 2. Section 803 of the New York city charter is amended by adding a new subdivision c-1 to read as follows:

c-1. The commissioner shall prepare annual audits of surveillance technology impact and use policies as defined in section 14-188 of the administrative code that shall:

1. assess whether the New York city police department's use of surveillance technology, as defined in section 14-188 of the administrative code, complies with the terms of the applicable surveillance technology impact and use policy;

2. describe any known or reasonably suspected violations of the surveillance technology impact and use

The New York City Council Page 3 of 4 Printed on 2/18/2021
powered by Legistar™



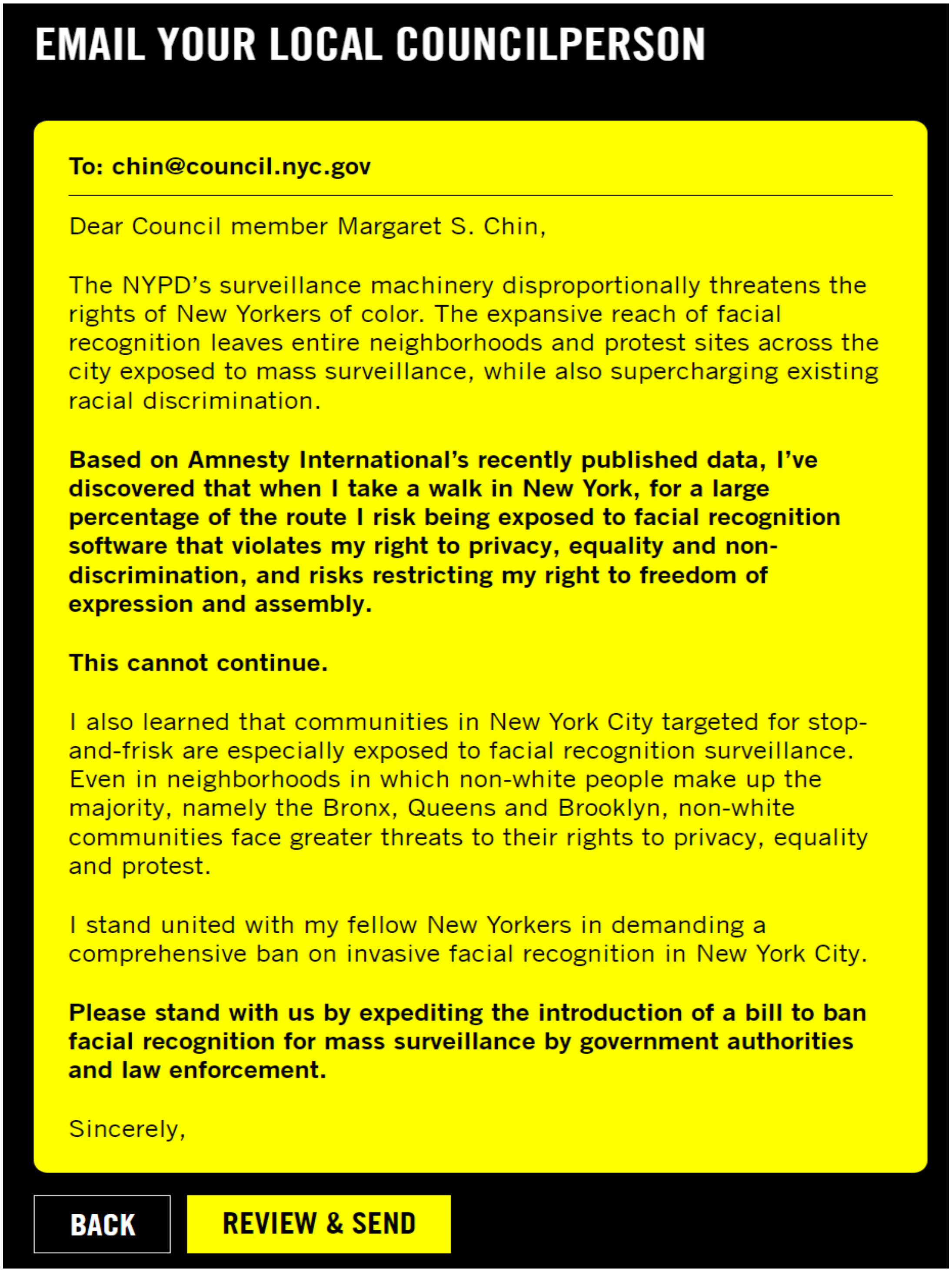
policy, including but not limited to complaints alleging such violations made by individuals pursuant to paragraph (6) of subdivision c of this section; and

3. publish recommendations, if any, relating to revisions of any surveillance technology impact and use policies.

§ 3. This local law takes effect immediately.

DA/BG
LS 6645/Int.1482-2017
LS 5531
6/10/20 10:40PM

## X. Appendix B: Example of Public Comment Template



EMAIL YOUR LOCAL COUNCILPERSON

**To: chin@council.nyc.gov**

Dear Council member Margaret S. Chin,

The NYPD's surveillance machinery disproportionally threatens the rights of New Yorkers of color. The expansive reach of facial recognition leaves entire neighborhoods and protest sites across the city exposed to mass surveillance, while also supercharging existing racial discrimination.

**Based on Amnesty International's recently published data, I've discovered that when I take a walk in New York, for a large percentage of the route I risk being exposed to facial recognition software that violates my right to privacy, equality and non-discrimination, and risks restricting my right to freedom of expression and assembly.**

**This cannot continue.**

I also learned that communities in New York City targeted for stop-and-frisk are especially exposed to facial recognition surveillance. Even in neighborhoods in which non-white people make up the majority, namely the Bronx, Queens and Brooklyn, non-white communities face greater threats to their rights to privacy, equality and protest.

I stand united with my fellow New Yorkers in demanding a comprehensive ban on invasive facial recognition in New York City.

**Please stand with us by expediting the introduction of a bill to ban facial recognition for mass surveillance by government authorities and law enforcement.**

Sincerely,

## XI. Appendix C: Text of NYPD's License Plate Readers IUP

**License Plate Readers IUP language, organized by section required by POST Act.**

Note: The blue blocked text in each section is repeated across multiple IUPs, as indicated by the below table.

| Percent of final 36 IUPs containing identical or nearly identical repetitions of blue blocked text | |
|---|---|
| Section | % |
| Capabilities of the Technology | No instances of boilerplate language (0%) |
| Rules, Processes & Guidelines Relating to Use | 83% |
| Safeguard & Security Measures Against Unauthorized Access | 92% |
| Policies & Procedures Relating to Retention, Access & Use of Data | 83% |
| Policies & Procedures Relating to Public Access or Use of Data | 94% |
| External Entities | 67% |
| Training | 75% |
| Internal Audit & Oversight Mechanisms | 64% |
| Health & Safety Reporting | 92% |
| Disparate Impacts of the IUP | 86% |

### Section 1: Capabilities of the surveillance technology

LPRs are specialized cameras that quickly capture images of license plate numbers affixed to vehicles that pass within the LPRs sensory range. An internal processor then converts the image of the license plate into a text the computer can process. This text is automatically compared against administrative databases containing enumerated lists of license plates of interest (i.e. stolen, wanted, etc.). LPRs are capable of properly functioning day or night, and in a variety of weather conditions.

NYPD makes use of two (2) kinds of LPRs: stationary and mobile. Stationary LPRs are permanently affixed to a specific location and record the license plates of all vehicles that pass within the LPR range. Mobile LPRs are attached to various NYPD vehicles and use the same technology to capture images of license plates the vehicle passes as it moves. Both stationary and mobile LPRs record a vehicle's license plate number and state of issuance, an [sic] images of a [sic] vehicle and the license plate, and the date, time and location the vehicle passed the LPR.

NYPD officers operating a NYPD vehicle imbedded with a NYPD tablet1 will receive an alert if the LPR scans a vehicle of interest, such as a vehicle reported stolen.

A limited number of authorized NYPD personnel can access a national commercial LPR data repository. LPR data obtained using NYPD LPRs or through the commercial repository cannot be used to track a vehicle in real-time.

NYPD LPRs do not use any biometric measurement technologies.

NOTE: No instances of repeated or boilerplate language was found in these sections.

**Section 2: Rules, Processes, & Guidelines Relating to Use of the Technology**

NYPD LPR policy seeks to balance the public safety benefits of this technology with individual privacy. LPRs [are used] in a manner consistent with the requirements and protection of the Constitution of the United States, the New York State Constitution, and applicable statutory authorities.

Court authorization is not sought prior to NYPD use of LPRs. Motor vehicles are heavily regulated by the government. The field-of-view of the LPRs utilized by NYPD is strictly limited to public areas and locations. LPRs capture images of license plates that are readily observable to any member of the public.

NYPD LPRs may only be used for legitimate law enforcement purposes. LPRs do not by themselves establish probable cause for an arrest, but provide NYPD investigators with valuable leads. NYPD limits authorized use of LPRs to the following circumstances: 1. Routine vehicle patrol; 2. Creation of alerts for specified complete or partial plate numbers; and 3. Capture movement of specified complete or partial plate numbers that momentarily pass the device.

In accordance with the Public Oversight of Surveillance Technology Act, an addendum to this [I]mpact and [U]se [P]olicy will be prepared as necessary to describe any additional uses of LPRs. NYPD investigations involving political activity are conducted by the Intelligence Bureau, which is the sole entity in the NYPD that may conduct investigations involving political activity pursuant to the Handschu Consent Decree.

No person will be the subject of police action solely because of actual or perceived race, color, religion or creed, age, national origin, alienage, citizenship status, gender (including gender identity), sexual orientation, disability, marital status, partnership status, military status, or political affiliation or beliefs.

The misuse of LPRs will subject employees to administrative and potentially criminal penalties.

NOTE: 30 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

### Section 3: Safeguard & Security Measures against Unauthorized Access

LPR data is accessible by using the NYPD Domain Awareness System (DAS)2. DAS is confidential-password-protected and access is restricted to only authorized users. Authorized users consist only of NYPD personnel in various commands, whose access has been requested by their commanding officer, and approved by the Information Technology Bureau (ITB).

DAS access is limited to authorized users who are authenticated by username and password. Access to DAS is limited to NYPD personnel with an articulable need to use the software in furtherance of a lawful duty. DAS access to LPR data is removed when access is no longer necessary for NYPD personnel to fulfill their duties (e.g., when personnel are transferred to a command that does not use the technology).

Access to the commercial repository is limited to authorized users who are authenticated by username and password. Access to the repository is limited to NYPD personnel with an articulable need to use the software in furtherance of a lawful duty. Access is removed when access is no longer necessary for NYPD personnel to fulfill their duties (e.g., when personnel are transferred to a command that does not use the technology).

LPR data can be downloaded and retained in an appropriate NYPD computer or case management system. Only authorized users have access to the data. NYPD personnel utilizing computer and case management systems are authenticated by username and password. Access to case management and computer systems is limited to personnel who have an articulable need to access the system in furtherance of lawful duty. Access rights within NYPD case management and computer systems are further limited based on lawful duty related to the official business of the NYPD. Access levels are only granted for functions and abilities relevant to individual commands.

The NYPD has a multifaceted approach to secure data and user accessibility within NYPD systems. 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. System security is one of many pillars incorporated into the EA process. Additionally, all NYPD computer systems are managed by a user permission hierarchy based on rank and role via Active Directory (AD) authentication. Passwords are never stored locally; user authentication is stored within the AD. The AD is managed by a Lightweight Directory Access Protocol (LDAP) to restrict/allow port access. Accessing NYPD computer systems remotely requires dual factor authentication. All data within NYPD computer systems are encrypted both in transit and at rest via Secure Socket Layer (SSL)/Transport Layer Security (TLS) certifications which follow industry best practices.

NYPD personnel must abide by security terms and conditions associated with computer and case management systems of the NYPD, including those governing user passwords and logon procedures. NYPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the NYPD, only as required in the execution of lawful duty.

NYPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to confidentiality policies may subject NYPD personnel to disciplinary and/or criminal action. NYPD personnel must confirm the identity and affiliation of individuals requesting information from the NYPD and determine that the release of information is lawful prior to disclosure.

Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

NOTE: 33 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

## Section 4: Policies & Procedures Relating to Retention, Access & Use of the Data

Data recorded by NYPD LPRs is accessible through DAS. All NYPD authorized users may only access DAS to execute their lawful duties by making official inquiries, which relate only to official business of the NYPD. Historical searches of LPR data may be conducted: 1. To determine if specified complete or partial plate numbers were detected by one or more fixed or mobile LPRs; 2. To identify all complete plate numbers detected by one or more fixed LPR during a specified time period; 3. To identify all complete plate numbers detected by a mobile LPR mounted on one or more specified vehicles during a specified time period; 4. To identify all complete plate numbers detected within a specified area during a specified time period; and 5. To identify preceding or subsequent complete plate numbers associated with one or more specified complete or partial plate numbers detected by one or more fixed or mobile LPRs in order to identify possible associates.

Data collected through NYPD's LPRs is retained for five (5) years. Access to the commercial LPR repository is critically limited and may only be accessed by select NYPD personnel for legitimate law enforcement purposes. The commercial repository will not be used unless there is an articulable reason to believe the queried vehicle has left the boundaries of NYC.

LPR data may only be used for legitimate law enforcement purposes or other official business of the NYPD, including in furtherance of criminal investigations, civil litigations, and disciplinary proceedings. Relevant data will be stored in an appropriate NYPD computer or case management system. NYPD personnel utilizing computer and case management systems are authenticated by username and password. Access to computer and case management is limited to personnel who have an articulable need to access the system in furtherance of lawful duty. Access rights within NYPD case management and computer systems are further limited based on lawful duty.

The Retention and Disposition Schedule for New York Local Government Records (the Schedule) establishes the minimum length of time local government agencies must retain their records before the records may be legally disposed.3 Published annually by the New York State Archives, the Schedule ensures compliance with State and Federal record retention requirements. The NYC Department of Records and Information Services (DORIS) publishes a supplemental records retention and disposition schedule (the Supplemental Schedule) in conjunction with the Law Department specifically for NYC agencies in order to satisfy business, legal, audit and legal requirements.

The retention period of a "case investigation record" depends on the classification of a case investigation record. The classification of case investigation records is based on the final disposition of the case, i.e., what the arrestee is convicted of or pleads to. Further, case investigations are not considered closed unless it results in prosecution and appeals are exhausted, it results in a settlement, it results in no arrest, or when restitution is no longer sought.

Case investigation records classified as a homicide, suicide, arson (first, second or third degree), missing person (until located), aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), active warrant, or stolen or missing firearms (until recovered or destroyed), must be retained permanently. Case investigation records classified as a fourth degree arson or non-fatal (including vehicular accidents) must be retained for a minimum of ten (10) years after the case is closed. Case investigation records classified as any other felony must be retained for a minimum of twenty-five (25) years after the case is closed. Case investigation records classified as a misdemeanor must be retained for a minimum of five (5) years after the case is closed. Case investigation records classified as a violation or traffic infraction must be retained for a minimum of one (1) year after the case is closed. Case investigation records classified as an offense against a child as defined by the Child Victims Act, excluding aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), must be retained until the child attains at least age fifty-five (55). Case investigation records connected to an investigation that reveals no offense has been committed by an adult must be kept for a minimum of five (5) years after the case is closed. Case investigation records connected to an investigation that reveals the individual involved was a juvenile and no arrest was made or no offense was committed must be kept for at least one (1) year after the juvenile attains age eighteen (18).

Personal information data files on criminals and suspects must be retained for at least five (5) years after the death of the criminal or suspect, or ninety (90) years after the criminal or suspect's date of birth as long as there has been no arrest in the last five (5) years, whichever is shorter. Personal 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.

The misuse of any data will subject employees to administrative and potentially criminal penalties.

NOTE: 30 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

### Section 5: Policies & Procedures Relating to Public Access or Use of the Data

Members of the public may request data obtained from the NYPD's use of LPRs pursuant to the New York State Freedom of Information Law. The NYPD will review and evaluate such requests in accordance with applicable provisions of law and NYPD policy.

NOTE: 34 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

### Section 6: External Entities

If a LPR obtains data related to a criminal case, the NYPD will turn the data over to the prosecutor with jurisdiction over the matter. Prosecutors will provide this data to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may LPR data (sic) from NYPD in accordance with applicable laws, regulations, and New York City and NYPD policies. Additionally, the NYPD may provide LPR data to partnering law enforcement and city agencies pursuant to on-going criminal investigations, civil litigation, and disciplinary proceedings. Information is not shared in furtherance of immigration enforcement.

Authorized agents within the state of New Jersey (NJ) have limited access to the NYPD LPR recorded data. Authorized agents of NJ law enforcement agencies are capable of conducting a search for pings of a specific license plate against NYPD owned or accessed LPR readers. However, NJ Authorized Agents do not have access to DAS.

Following the laws of the State and City of New York, as well as NYPD policy, information stemming from LPR use may be provided to community leaders, civic organizations and the news media in order to further an investigation, create awareness of an unusual incident, or address a community-concern.

Pursuant to NYPD policy and local law, NYPD personnel may disclose identifying information externally only if:

1. Such disclosure has been authorized in writing by the individual to whom such information pertains to, or if such individual is a minor or is otherwise not legally competent, by such individual's parent or legal guardian and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau; 2. Such disclosure is required by law and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau; 3. Such disclosure furthers the purpose or mission of the NYPD and has been approved in writing by the Agency Privacy Officer

assigned to the Legal Bureau; 4. Such disclosure has been pre-approved as in the best interests of the City by the City Chief Privacy Officer; 5. Such disclosure has been designated as routine by the Agency Privacy Officer assigned to the Legal Bureau; 6. Such disclosure is in connection with an investigation of a crime that has been committed or credible information about an attempted or impending crime; 7. Such disclosure is in connection with an open investigation by a City agency concerning the welfare of a minor or an individual who is otherwise not legally competent.

Government 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. Such access is granted by the NYPD on a case by case basis subject to the terms of written agreements between the NYPD and the agency receiving access to a specified system. The terms of the written agreements also charge these external entities with maintaining the security and confidentiality of information obtained from the NYPD, limiting disclosure of that information without NYPD approval, and notifying the NYPD when the external entity receives a request for that information pursuant to a subpoena, judicial order, or other legal process. Access will not be given to other agencies for purposes of furthering immigration enforcement.

The NYPD purchases LPRs and associated equipment or Software as a Service (SaaS)/software from approved vendors. The NYPD emphasizes the importance of and engages with vendors and contractors to maintain the confidentiality, availability, and integrity of NYPD technology systems.

Vendors and contractors may have access to NYPD LPRs associated software or data in the performance of contractual duties to the NYPD. Such duties are typically technical or proprietary in nature (e.g., maintenance or failure mitigation). In providing vendors and contractors access to equipment and computer systems, the NYPD follows the principle of least privilege. Vendors and contractors are only allowed access on a "need to know basis" to fulfill contractual obligations and/or agreements.

Vendors and contractors providing equipment and services to the NYPD undergo vendor responsibility determination and integrity reviews. Vendors and contractors providing sensitive equipment and services to the NYPD also undergo background checks.

Vendors and contractors are legally obligated by contracts and/or agreements to maintain the confidentiality of NYPD data and information. Vendors and contractors are subject to criminal and civil penalties for unauthorized use or disclosure of NYPD data or information.

If LPR data is disclosed in a manner violating the local Identifying Information Law, the NYPD Agency Privacy Officer, upon becoming aware, must report the disclosure to the NYC Chief Privacy Officer as soon as practicable. The NYPD must make reasonable efforts to notify individuals effected by the disclosure in writing when there is potential risk of harm to the individual, when the NYPD determines in consultation with the NYC Chief Privacy Officer and the Law Department that notification should occur, or when legally required to do so by law or regulation. In accordance with the Identifying Information Law, the NYC Chief Privacy Officer submits a quarterly report containing an anonymized compilation or summary of such disclosures by City agencies, including those reported by the NYPD, to the Speaker of the Council and makes the report publically available online.

NOTE: 24 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

### Section 7: Training

NYPD officers using LPRs receive command level training on the proper operation of the technology and associated equipment. Officers must operate NYPD LPRs in compliance with NYPD policies and training.

NOTE: 27 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

### Section 8: Internal Audit & Oversight Mechanisms

Supervisors of personnel utilizing LPRs are responsible for security and proper utilization of the technology and associated equipment. Supervisors are directed to inspect all areas containing NYPD computer systems at least once each tour and ensure that all systems are being used within NYPD guidelines.

Any search conducted in DAS relating to LPR associated information is auditable by ITB.

All NYPD personnel are advised that NYPD computer systems and equipment are intended for the purposes of conducting official business. The misuse of any system or equipment will subject employees to administrative and potentially criminal penalties. Allegations of misuse are internally investigated at the command level or by the NYPD Internal Affairs Bureau (IAB).

Integrity Control Officers (ICOs) within each Command are responsible for maintaining the security and integrity of all recorded media in the possession of the NYPD. ICOs must ensure all authorized users of NYPD computer systems in their command understand and comply with computer security guidelines, frequently observe all areas with computer equipment, and ensure security guidelines are complied with, as well as investigating any circumstances or conditions which may indicate abuse of the computer systems.

Requests for focused audits of computer activity from IAB, Commanding Officers, ICOs, Investigations Units, and others, may be made to the Information Technology Bureau.

NOTE: 23 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

### Section 9: Health & Safety Reporting

There are no known health and safety issues with LPRs or associated equipment.

NOTE: 33 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

### Section 10: Disparate Impacts of the Impact & Use Policy

The safeguards and audit protocols built into this [I]mpact and [U]se [P]olicy for LPRs mitigate the risk of impartial [sic] and biased law enforcement. LPRs capture images of vehicle license plates utilizing NYC's public roadways. LPRs do not use any biometric measurement technologies.

The 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. Should an officer initiates enforcement action against a person, motivated even in part by a person's actual or perceived race, color, ethnicity, or national origin, that enforcement action violates NYPD policy unless the officer's decision is based on a specific and reliable suspect description that includes not only race, age, and gender, but other identifying characteristics or information.

NOTE: 31 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

## XII. Appendix D: Text of NYPD's Social Network Analysis Tools IUP

### Section 1: Capabilities of the Technology

NYPD social network analysis tools process information on social networking platforms to aid personnel in discovering information relevant to investigations and to address public safety concerns. For example, in the aftermath of a terrorist attack committed outside of New York City, the NYPD may use social network analysis tools to quickly assess the social media profile of the perpetrator for connections to the New York City area and allocate resources in response.

Similarly, social network analysis tools assist the NYPD in addressing criminal activity in New York City. When investigating an assault committed by multiple subjects, social network analysis tools can reveal investigative leads by highlighting otherwise unknown connections between the subjects acting in concert.

However, the NYPD may miss information critical to investigations because users can easily remove information posted on social media and social media platforms routinely delete content and deactivate accounts for violations of terms of service. Accordingly, social network analysis tools allow the NYPD to retain information on social networking platforms relevant to investigations and alert investigators to new activity on queried social media accounts.

Information accessible to NYPD personnel using social network analysis tools is limited to publicly available information, or information that is viewable as a result of user privacy settings or practices. Publically available images may be downloaded and may be used a probe image for facial recognition analysis.1 Social network analysis tools cannot be used for computer hacking, do not perform facial recognition and do not use any other biometric measuring technologies.

### Section 2: Rules, Processes & Guidelines Relating to Use of The Technology

NYPD social network analysis tools policy seeks to balance the public safety benefits of this technology with individual privacy. The NYPD must use social network analysis tools in a manner consistent with the requirements and protection of the

Constitution of the United States, the New York State Constitution, and applicable statutory authorities.

Social network analysis tools may only be used for legitimate law enforcement purposes. Information identified by using social network analysis tools does not by itself establish probable cause to arrest or obtain a search warrant. However, it may generate leads for further investigation.

The NYPD does not seek court authorization prior to using social network analysis tools. The processed information is limited to publicly available information or information that is viewable as a result of user-selected privacy settings or practices.

In accordance with the Public Oversight of Surveillance Technology Act, an addendum to this impact and use policy will be prepared as necessary to describe any additional uses of social network analysis tools.

NYPD investigations involving political activity are conducted by the Intelligence Bureau, which is the sole entity in the NYPD that may conduct investigations involving political activity pursuant to the *Handschu* Consent Decree.

No person will be the subject of police activity solely because of actual or perceived race, color, religion or creed, age, national origin, alienage, citizenship status, gender (including gender identity), sexual orientation, disability, marital status, partnership status, military status, or political affiliation or beliefs.

The misuse of social network analysis tools will subject employees to administrative and potentially criminal penalties.

### Section 3: Safeguard & Security Measures Against Unauthorized Access

Access to social network analysis tools is critically limited. Authorized users are authenticated by username and password. Account credentials for social network analysis tools must be securely maintained and stored at all times. Access to social network analysis tools is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to NYPD social network analysis tools is removed when the technology is no longer necessary for NYPD personnel to fulfill their duties (e.g., when personnel are transferred to a command that does not use the technology).

Information obtained from NYPD social network analysis tools are retained within an appropriate case management or computer systems. Only authorized users have access to these recordings. NYPD personnel utilizing computer and case management systems are authenticated by username and password. Access to case management and computer systems is limited to personnel who have an articulable need to access the system in furtherance of lawful duty. Access rights within NYPD case management and computer systems are further limited based on lawful duty. Authorized users can only access data and perform tasks allocated to them by the system administrator according to their role.

The NYPD has a multifaceted approach to secure data and user accessibility within NYPD systems. 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. System security is one of many pillars incorporated into the EA process. Additionally, all NYPD computer systems are managed by a user permission hierarchy based on rank and role via Active Directory (AD) authentication. Passwords are never stored locally; user authentication is stored within the AD. The AD is managed by a Lightweight Directory Access Protocol (LDAP) to restrict/allow port access. Accessing NYPD computer systems remotely requires dual factor authentication. All data within NYPD computer systems are encrypted both in transit and at rest via Secure Socket Layer (SSL)/Transport Layer Security (TLS) certifications which follow industry best practices.

NYPD personnel must abide by security terms and conditions associated with computer and case management systems of the NYPD, including those governing user passwords and logon procedures. Members of the NYPD must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the NYPD, only as required in the execution of lawful duty.

NYPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to confidentiality policies may subject NYPD personnel to disciplinary and/or criminal action. NYPD personnel must confirm the identity and affiliation of individuals requesting information from the NYPD and determine that the release of information is lawful prior to disclosure.

Unauthorized access to any system will subject employees to administrative and potentially criminal penalties.

### Section 4: Policies & Procedures Relating to Retention, Access, & Use of The Data

Information obtained from social network analysis tools may only be used for legitimate law enforcement purposes or official business of the NYPD, including in furtherance of criminal investigations, civil litigations, and disciplinary proceedings. Information relevant to a case or investigation is stored electronically in an appropriate NYPD case management and computer system. NYPD personnel utilizing case management and computer systems are authenticated by username and password. Access to case management and computer systems is limited to personnel who have an articulable need to access the system in furtherance of lawful duty. Access rights within NYPD case management and computer systems are further limited based on lawful duty.

The Retention and Disposition Schedule for New York Local Government Records (the Schedule) establishes the minimum length of time local government agencies must retain their records before the records may be legally disposed.2 Published annually by the New York State Archives, the Schedule ensures compliance with State and Federal record retention requirements. The NYC Department of Records and Information Services (DORIS) publishes a supplemental records retention and disposition schedule (the Supplemental Schedule) in conjunction with the Law Department specifically for NYC agencies in order to satisfy business, legal, audit and legal requirements.3

The retention period of a "case investigation record" depends on the classification of a case investigation record. The classification of case investigation records is based on the final disposition of the case, i.e., what the arrestee is convicted of or pleads to. Further, case investigations are not considered closed unless it results in prosecution and appeals are exhausted, it results in a settlement, it results in no arrest, or when restitution is no longer sought.

Case investigation records classified as a homicide, suicide, arson (first, second or third degree), missing person (until located), aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), active warrant, or stolen or missing firearms (until recovered or destroyed), must be retained permanently. Case investigation records classified as a fourth degree arson or non-fatal (including vehicular accidents) must be retained for a minimum of ten (10) years after the case is closed. Case investigation records classified as any other felony must be retained for a minimum of twenty-five (25) years after the case is closed. Case investigation records classified as a misdemeanor must be retained for a minimum of five (5) years after the case is closed. Case investigation records classified as a violation or traffic infraction must be retained for a minimum of one (1) year after the case is closed. Case investigation records classified as an offense against a child as defined by the Child Victims Act, excluding aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), must be retained until the child attains at least age fifty-five (55). Case investigation records connected to an investigation that reveals no offense has been committed by an adult must be kept for a minimum of five (5) years after the case is closed. Case investigation records connected to an investigation that reveals the individual involved was a juvenile and no arrest was made or no offense was committed must be kept for at least one (1) year after the juvenile attains age eighteen (18).

Personal information data files on criminals and suspects must be retained for at least five (5) years after the death of the criminal or suspect, or ninety (90) years after the criminal or suspect's date of birth as long as there has been no arrest in the last five (5) years, whichever is shorter. Personal 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.

The misuse of any system will subject employees to administrative and potentially criminal penalties.

### Section 5: Policies & Procedures Relating to Public Access or Use of The Data

Members of the public may request information obtained from NYPD use of social network analysis tools pursuant to the New York State Freedom of Information Law. The NYPD will review and evaluate such requests in accordance with applicable provisions of law and NYPD policy.

### Section 6: External Entities

If the use of social network analysis tools yields information relevant to a criminal case, the NYPD will share it with the prosecutor with jurisdiction over the matter. Prosecutors will provide the information to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may request information contained in NYPD computer or case management systems in accordance with applicable laws, regulations, and New York City and NYPD policies. Additionally, the NYPD may provide the information or details related to it to partnering law enforcement and city agencies pursuant to on-going criminal investigations, civil litigation, and disciplinary proceedings. Information is not shared in furtherance of immigration enforcement.

Following the laws of the State and City of New York, as well as NYPD policy, the information related to social network analysis may be provided to community leaders, civic organizations and the news media in order to further an investigation, create awareness of an unusual incident, or address a community-concern. Pursuant to NYPD policy and local law, NYPD personnel may disclose identifying information externally only if:

1. Such disclosure has been authorized in writing by the individual to whom such information pertains to, or if such individual is a minor or is otherwise not legally competent, by such individual's parent or legal guardian and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;

2. Such disclosure is required by law and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;

3. Such disclosure furthers the purpose or mission of the NYPD and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;

4. Such disclosure has been pre-approved as in the best interests of the City by the City Chief Privacy Officer;

5. Such disclosure has been designated as routine by the Agency Privacy Officer assigned to the Legal Bureau;

6. Such disclosure is in connection with an investigation of a crime that has been committed or credible information about an attempted or impending crime; or

7. Such disclosure is in connection with an open investigation by a City agency concerning the welfare of a minor or an individual who is otherwise not legally competent.

Government 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. Such access is granted by the NYPD on a case by case basis subject to the terms of written agreements between the NYPD and the agency receiving access to a specified system. The terms of the written agreements also charge these external entities with maintaining the security and confidentiality of information obtained from the NYPD, limiting disclosure of that information without NYPD approval, and notifying the NYPD when the external entity receives a request for that information pursuant to a subpoena, judicial order, or other legal process. Access will not be given to other agencies for purposes of furthering immigration enforcement.

The NYPD purchases social network analysis tools and associated equipment or Software as a Service (SaaS)/software from approved vendors. The NYPD emphasizes the importance of and engages with vendors and contractors to maintain the confidentiality, availability, and integrity of NYPD technology systems.

Vendors and contractors may have access to NYPD social network analysis tools associated software or data in the performance of contractual duties to the NYPD. Such duties are typically technical or proprietary in nature (e.g., maintenance or failure mitigation). In providing vendors and contractors access to equipment and computer systems, the NYPD follows the principle of least privilege. Vendors and contractors are only allowed access on a "need to know basis" to fulfill contractual obligations and/or agreements.

Vendors and contractors providing equipment and services to the NYPD undergo vendor responsibility determination and integrity reviews. Vendors and contractors providing sensitive equipment and services to the NYPD also undergo background checks.

Vendors and contractors are legally obligated by contracts and/or agreements to maintain the confidentiality of NYPD data and information. Vendors and contractors are subject to criminal and civil penalties for unauthorized use or disclosure of NYPD data or information.

If information obtained using NYPD social network analysis tools is disclosed in a manner violating the local Identifying Information Law, the NYPD Agency Privacy Officer, upon becoming aware, must report the disclosure to the NYC Chief Privacy Officer as soon as practicable. The NYPD must make reasonable efforts to notify individuals effected by the disclosure in writing when there is potential risk of harm to the individual, when the NYPD determines in consultation with the NYC Chief Privacy Officer and the Law Department that notification should occur, or when legally required to do so by law or regulation. In accordance with the Identifying Information Law, the NYC Chief Privacy Officer submits a quarterly report containing an anonymized compilation or summary of such disclosures by City agencies, including those reported by the NYPD, to the Speaker of the Council and makes the report publically available online.

### Section 7: Training

NYPD personnel using social network analysis tools receive command level training on the proper operation of the technology and associated equipment. All NYPD personnel must use social network analysis tools in compliance with NYPD policies and training.

### Section 8: Internal Audit & Oversight Mechanisms

Supervisors of personnel utilizing social network analysis tools are responsible for security and proper utilization of the technology and associated equipment. Supervisors are directed to inspect all areas containing NYPD computer systems at least once each tour and ensure that all systems are being used within NYPD guidelines.

All NYPD personnel are advised that NYPD computer systems and equipment are intended for the purposes of conducting official business. The misuse of any system or equipment will subject employees to administrative and potentially criminal penalties. Allegations of misuse are internally investigated at the command level or by the Internal Affairs Bureau (IAB).

Integrity Control Officers (ICOs) within each Command are responsible for maintaining the security and integrity of all recorded media in the possession of the NYPD. ICOs must ensure all authorized users of NYPD computer systems in their command understand and comply with computer security guidelines, frequently observe all areas with computer equipment, and ensure security guidelines are complied with, as well as investigating any circumstances or conditions which may indicate abuse of the computer systems.

Requests for focused audits of computer activity from IAB, Commanding Officers, ICOs, Investigations Units, and others, may be made to the Information Technology Bureau.

**Section 9: Health & Safety Reporting**

There are no known health and safety issues with social network analysis tools or the associated equipment.

**Section 10: Disparate Impacts of the Impact & Use Policy**

The safeguards and audit protocols built into this impact and use policy for NYPD social network analysis tools mitigate the risk of impartial [sic] and biased law enforcement. Social network analysis tools are only capable of processing information a user chooses to share on social networking platforms. NYPD social network analysis tools do not use any biometric measurement technologies.

The 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. When an officer's decision to initiate enforcement action against a person is motivated even in part by a person's actual or perceived race, color, ethnicity, or national origin, that enforcement action violates NYPD policy unless the officer's decision is based on a specific and reliable suspect description that includes not just race, age, and gender, but other identifying characteristics or information.

## XIII. Appendix E: Text of NYPD's Facial Recognition IUP

### Section 1: Capabilities of the Technology

Since 2011, the NYPD has successfully used facial recognition technology to investigate criminal activity and increase public safety. The NYPD uses facial recognition to aid in the identification of suspects whose images have been recorded on-camera at robberies, burglaries, assaults, shootings, and other serious crimes. The NYPD also uses facial recognition to aid in the identification of persons unable to identify themselves (e.g., persons experiencing memory loss or unidentified deceased persons).

NYPD investigators often obtain video and photo over the course of an investigation. If a video or photo contains an image of a face of an unknown individual, the image can be submitted for facial recognition analysis in accordance with NYPD facial recognition policy.

Known as a probe image, NYPD facial recognition software compares the image to a controlled and limited group of photos already within lawful possession of the NYPD, called the photo repository. The photo repository only contains arrest and parole photographs of individuals that have been charged with a crime where criminal court has jurisdiction. Probe images are never entered into and do not become part of the photo repository.

NYPD facial recognition technology analyzes one probe image at a time. The software generates a pool of possible match candidates that are manually reviewed by specially trained NYPD facial recognition investigators to determine the differences and similarities between a probe image and a potential match.

The NYPD does not integrate facial recognition technology with any NYPD video cameras or systems (e.g., CCTV cameras, unmanned aircraft systems, and body worn cameras) for real-time facial recognition analysis. The NYPD does not have a capability for real-time facial recognition.

Facial recognition technology does not use any additional biometric measuring technologies.

### Section 2: Rules, Processes & Guidelines Relating to Use of The Technology

NYPD facial recognition policy seeks to balance the public safety benefits of this technology with individual privacy. Facial recognition technology must be used in a manner consistent with the requirements and protection of the Constitution of the United States, the New York State Constitution, and applicable statutory authorities.

The facial recognition process does not by itself establish a basis for a stop, probable cause to arrest, or to obtain a search warrant. However, it may generate investigative leads through a combination of automated biometric comparisons and human analysis.

Facial recognition technology must only be used for legitimate law enforcement purposes. Authorized uses of facial recognition technology are limited to the following:

1. To identify an individual when there is a basis to believe that such individual has committed, is committing, or is about to commit a crime;

2. To identify an individual when there is a basis to believe that such individual is a missing person, crime victim, or witness to criminal activity;

3. To identify a deceased person;

4. To identify a person who is incapacitated or otherwise unable to identify themselves;

5. To identify an individual who is under arrest and does not possess valid identification, is not forthcoming with valid identification, or who appears to be using someone else's identification, or a false identification; or

6. To mitigate an imminent threat to health or public safety (e.g., to thwart an active terrorism scheme or plot).

For criminal investigations, a possible facial recognition match serves as a lead for additional steps. An arrest will not be made until the assigned investigator establishes, with other corroborating evidence, that the suspect identified as a possible match is the perpetrator in an alleged crime.

When an investigator obtains an image depicting the face of an unidentified suspect, victim, or witness, and intends to identify the individual using facial recognition technology, the investigator must submit a request for facial recognition analysis. Specifically, the request is made for the image depicting the face of the unknown person (the probe image) to be compared to photos in the NYPD arrest and parole photo repository. The request for facial recognition analysis must include a case or complaint number for the matter under investigation and the probe image(s) of the unidentified person.

The facial recognition investigator must confirm the basis of the request is in compliance with the enumerated list authorized uses of facial recognition technology. That confirmation must be documented by the requesting investigator in an appropriate NYPD case management system. The facial recognition investigator will select a probe image of the unidentified person from the submitted images. If image quality is unsuitable for facial recognition comparison, the requesting investigator will be notified and given the opportunity to submit additional images.

The facial recognition investigator will run a search using a facial recognition software for comparison of the probe image to images lawfully obtained by the NYPD. The software generates a pool of possible match candidates.

If a possible match candidate is identified, the facial recognition investigator must then manually review and analyze each result. This process, known as facial identification, consists of visual comparison of the facial characteristics of each candidate against the probe image. Comparisons are made with regard to various facial features such as the eyes, ears, nose, mouth, chin, lips, eyebrows, hair/hairline, scars, marks, and tattoos. A detailed background check is conducted by the facial recognition investigator to corroborate a possible match.

Next, a possible match candidate is submitted for peer review by other facial recognition investigators. A supervisor of the facial recognition investigator performs a final review of a possible match candidate and provides final approves, if appropriate.

If there is a difference of opinion with the findings, the supervisor will direct personnel to continue investigation for a possible match candidate. A report of negative results will be provided to the requesting investigator if a possible match candidate is not identified or approved by the supervisor.

If a possible match candidate is approved, the facial recognition investigator will prepare a possible match report and attach it to the requesting investigator's case file in the case management system. The possible match report includes the probe image, a notification stating that the determination of a possible match candidate alone does not constitute probable cause to effect an arrest or obtain an arrest or search warrant, and that further investigation is needed to establish probable cause.

Images obtained from body-worn cameras worn by NYPD officers are not routinely submitted for facial recognition analysis. For example, the NYPD does not use facial recognition technology to examine body-worn camera video to identify people who may have open warrants. However, if an officer, whose body-worn camera is activated, witnesses a crime but is unable to apprehend the suspect, a still image of the suspect may be extracted from body-worn camera video and submitted for facial recognition analysis.

The NYPD does not use facial recognition technology to monitor and identify people in crowds or political rallies.

The NYPD does not seek court authorization prior to the use of facial recognition technology since the tool conducts analysis of images that have been lawfully-obtained by the NYPD.

The use of facial recognition technology that compares probe images against images outside the photo repository is prohibited unless approval is granted for such analysis in a specific case for an articulable reason by the Chief of Detectives or Deputy Commissioner, Intelligence and Counterterrorism.

In situations where use of a NYPD facial recognition technology has not been foreseen or prescribed in policy, the Chief of Detectives or Deputy Commissioner of Intelligence and Counterterrorism, will decide if use is appropriate and lawful. In accordance with the Public Oversight of Surveillance Technology Act, an addendum to this impact and use policy will be prepared as necessary to describe any additional uses of facial recognition technology.

NYPD investigations involving political activity are conducted by the Intelligence Bureau, which is the sole entity in the NYPD that may conduct investigations involving political activity pursuant to the *Handschu* Consent Decree.

No person will be the subject of police action solely because of actual or perceived race, color, religion or creed, age, national origin, alienage, citizenship status, gender (including gender identity), sexual orientation, disability, marital status, partnership status, military status, or political affiliation or beliefs.

The misuse of facial recognition technology will subject employees to administrative and potentially criminal penalties.

### Section 3: Safeguard & Security Measures Against Unauthorized Access

Access to facial recognition technology is limited to NYPD facial recognition investigators. Access to facial recognition technology is removed when the technology is no longer necessary for NYPD personnel to fulfill their duties (e.g., when facial recognition investigators are transferred to a different command).

Facial recognition investigators using the software are first authenticated by username and password. Facial recognition investigators are provided with access only after completing mandatory training related to use of the technology.

Information resulting from use of facial recognition technology is retained within NYPD computer and case management systems. NYPD personnel utilizing computer and case management systems are authenticated by username and password. Access to case management and computer systems is limited to personnel who have an articulable need to access the system in furtherance of lawful duty. Access rights within NYPD case management and computer systems are further limited based on lawful duty. Authorized users can only access data and perform tasks allocated to them by the system administrator according to their role.

The NYPD has a multifaceted approach to secure data and user accessibility within NYPD systems. 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. System security is one of many pillars incorporated into the EA process. Additionally, all NYPD computer systems are managed by a user permission hierarchy based on rank and role via Active Directory (AD) authentication. Passwords are never stored locally; user authentication is stored within the AD. The AD is managed by a Lightweight Directory Access Protocol (LDAP) to restrict/allow port access. Accessing NYPD computer systems remotely requires dual factor authentication. All data within NYPD computer systems are encrypted both in transit and at rest via Secure Socket Layer (SSL)/Transport Layer Security (TLS) certifications which follow industry best practices.

NYPD personnel must abide by security terms and conditions associated with computer and case management systems of the NYPD, including those governing user passwords and logon procedures. NYPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the NYPD, only as required in the execution of lawful duty.

NYPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to confidentiality policies may subject NYPD personnel to disciplinary and/or criminal action. NYPD personnel must confirm the identity and affiliation of individuals requesting information from the NYPD and determine that the release of information is lawful prior to disclosure.

Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

### Section 4: Policies & Procedures Relating to Retention, Access, & Use of The Data

The results of facial recognition analysis may only be used for legitimate law enforcement purposes or other official business of the NYPD, including in furtherance of criminal investigations, civil litigations, and disciplinary proceedings. Facial recognition analysis results relevant to a case or investigation are stored in appropriate NYPD computer or case management systems. These results NYPD personnel utilizing computer and case management systems are authenticated by username and password. Access to computer and case management is limited to personnel who have an articulable need to access the system in furtherance of lawful duty.

The Retention and Disposition Schedule for New York Local Government Records (the Schedule) establishes the minimum length of time local government agencies must retain their records before the records may be legally disposed.1 Published annually by the New York State Archives, the Schedule ensures compliance with State and Federal record retention requirements. The NYC Department of Records and Information Services (DORIS) publishes a supplemental records retention and disposition schedule (the Supplemental Schedule) in conjunction with the Law Department specifically for NYC agencies in order to satisfy business, legal, audit and legal requirements.2

The retention period of a "case investigation record" depends on the classification of a case investigation record. The classification of case investigation records is based on the final disposition of the case, i.e., what the arrestee is convicted of or pleads to. Further, case investigations are not considered closed unless it results in prosecution and appeals are exhausted, it results in a settlement, it results in no arrest, or when restitution is no longer sought.

Case investigation records classified as a homicide, suicide, arson (first, second or third degree), missing person (until located), aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), active warrant, or stolen or missing firearms (until recovered or destroyed), must be retained permanently. Case investigation records classified as a fourth degree arson or non-fatal (including vehicular accidents) must be retained for a minimum of ten (10) years after the case is closed. Case investigation records classified as any other felony must be retained for a minimum of twenty-five (25) years after the case is closed. Case investigation records classified as a misdemeanor must be retained for a minimum of five (5) years after the case is closed. Case investigation records classified as a violation or traffic infraction must be retained for a minimum of one (1) year after the case is closed. Case investigation records classified as an offense against a child as defined by the Child Victims Act, excluding aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), must be retained until the child attains at least age fifty-five (55). Case investigation records connected to an investigation that reveals no offense has been committed by an adult must be kept for a minimum of five (5) years after the case is closed. Case investigation records connected to an investigation that reveals the individual involved was a juvenile and no arrest was made or no offense was committed must be kept for at least one (1) year after the juvenile attains age eighteen (18).

Personal information data files on criminals and suspects must be retained for at least five (5) years after the death of the criminal or suspect, or ninety (90) years after the criminal or suspect's date of birth as long as there has been no arrest in the last five (5) years, whichever is shorter. Personal 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.

The misuse of information will subject employees to administrative and potentially criminal penalties.

### Section 5: Policies & Procedures Relating to Public Access or Use of The Data

Members of the public may request information obtained from the NYPD use of facial recognition technology pursuant to the New York State Freedom of Information Law. The NYPD will review and evaluate such requests in accordance with applicable provisions of law and NYPD policy.

### Section 6: Eternal Entities

If the use of facial recognition technology produces information related to a criminal case, the NYPD will turn it over to the prosecutor with jurisdiction over the matter. Prosecutors will provide the information to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may request information contained in NYPD computer or case management systems in accordance with applicable laws, regulations, and New York City and NYPD policies. Additionally, the NYPD may provide information to partnering law enforcement and city agencies pursuant to on-going criminal investigations, civil litigation, and disciplinary proceedings. Such information will not be shared in furtherance of immigration enforcement.

Following the laws of the State and City of New York, as well as NYPD policy, information stemming from facial recognition technology may be provided to community leaders, civic organizations and the news media in order to further an investigation, create awareness of an unusual incident, or address a community-concern.

Pursuant to NYPD policy and local law, NYPD personnel may disclose identifying information externally only if:

1. Such disclosure has been authorized in writing by the individual to whom such information pertains to, or if such individual is a minor or is otherwise not legally competent, by such individual's parent or legal guardian and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;

2. Such disclosure is required by law and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;

3. Such disclosure furthers the purpose or mission of the NYPD and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;

4. Such disclosure has been pre-approved as in the best interests of the City by the City Chief Privacy Officer;

5. Such disclosure has been designated as routine by the Agency Privacy Officer assigned to the Legal Bureau;

6. Such disclosure is in connection with an investigation of a crime that has been committed or credible information about an attempted or impending crime;

7. Such disclosure is in connection with an open investigation by a City agency concerning the welfare of a minor or an individual who is otherwise not legally competent.

Government 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. Such access is granted by the NYPD on a case by case basis subject to the terms of written agreements between the NYPD and the agency receiving access to a specified system. The terms of the written agreements also charge these external entities with maintaining the security and confidentiality of information obtained from the NYPD, limiting disclosure of that information without NYPD approval, and notifying the NYPD when the external entity receives a request for that information pursuant to a subpoena, judicial order, or other legal process. Access will not be given to other agencies for purposes of furthering immigration enforcement.

The NYPD purchases facial recognition technology and associated equipment or Software as a Service (SaaS)/software from approved vendors. The NYPD emphasizes the importance of and engages with vendors and contractors to maintain the confidentiality, availability, and integrity of NYPD technology systems.

Vendors and contractors may have access to NYPD facial recognition technology associated program or data in the performance of contractual duties to the NYPD. Such duties are typically technical or proprietary in nature (e.g., maintenance or failure mitigation). In providing vendors and contractors access to equipment and computer systems, the NYPD follows the principle of least privilege. Vendors and contractors are only allowed access on a "need to know basis" to fulfill contractual obligations and/or agreements.

Vendors and contractors providing equipment and services to the NYPD undergo vendor responsibility determination and integrity reviews. Vendors and contractors providing sensitive equipment and services to the NYPD also undergo background checks.

Vendors and contractors are legally obligated by contracts and/or agreements to maintain the confidentiality of NYPD data and information. Vendors and contractors are subject to criminal and civil penalties for unauthorized use or disclosure of NYPD data or information. If facial recognition data is disclosed in a manner violating the local Identifying Information Law, the NYPD Agency Privacy Officer, upon becoming aware, must report the disclosure to the NYC Chief Privacy Officer as soon as practicable. The NYPD must make reasonable efforts to notify individuals effected by the disclosure in writing when there is potential risk of harm to the individual, when the NYPD determines in consultation with the NYC Chief Privacy Officer and the Law Department that notification should occur, or when legally required to do so by law or regulation. In accordance with the Identifying Information Law, the NYC Chief Privacy Officer submits a quarterly report containing an anonymized compilation or summary of such disclosures by City agencies, including those reported by the NYPD, to the Speaker of the Council and makes the report publically available online.

### Section 7: Training

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.

### Section 8: Internal Audit & Oversight Mechanisms

The use of facial recognition technology, including the reasons for its use, must be discussed with a supervisor. Supervisors of personnel utilizing facial recognition technology are responsible for security and proper utilization of the technology and associated equipment. Supervisors are directed to inspect all areas containing NYPD computer systems at least once each tour and ensure that all systems are being used within NYPD guidelines.

All NYPD personnel are advised that NYPD computer systems and equipment are intended for the purposes of conducting official business. The misuse of any system or equipment will subject employees to administrative and potentially criminal penalties. Allegations of misuse are internally investigated at the command level or by the Internal Affairs Bureau (IAB).

Integrity Control Officers (ICOs) within each Command are responsible for maintaining the security and integrity of all recorded media in the possession of the NYPD. ICOs must ensure all authorized users of NYPD computer systems in their command understand and comply with computer security guidelines, frequently observe all areas with computer equipment, and ensure security guidelines are complied with, as well as investigating any circumstances or conditions which may indicate abuse of the computer systems.

Requests for focused audits of computer activity from IAB, Commanding Officers, ICOs, Investigations Units, and others, may be made to the Information Technology Bureau.

**Section 9: Health & Safety Reporting**

There are no known health and safety issues with facial recognition technologies or associated equipment.

**Section 10: Disparate Impacts of The Impact & Use Policy**

The safeguards and audit protocols built into this impact and use policy for facial recognition technology mitigate the risk of impartial [sic] and biased law enforcement. NYPD facial recognition policy integrates human investigators in all phases. All possible facial recognition matches undergo a peer review by other facial recognition investigators. Further, the possible match report includes the probe image, a notification stating that the determination of a possible match candidate alone does not constitute probable cause to effect an arrest or obtain an arrest or search warrant, and that further investigation is needed to establish probable cause.

Some studies have found variations in accuracy for some software products in analyzing the faces of African Americans, Asians Americans, women, and groups other than non-white males. However, an important federal government study on the subject noted that in "hybrid machine/human systems," where the software findings are routinely reviewed by human investigators, erroneous software matches can be swiftly corrected by human observers.

Facial recognition technology utilizes algorithms in order to identify possible match candidates to a probe image. The NYPD only uses facial recognition algorithms which have been evaluated by the National Institute of Standards and Technology (NIST) for matching efficiency and accuracy, which includes an evaluation of the accuracy of the algorithm across demographics. Algorithms utilized for facial recognition are periodically updated as necessary based on subsequent NIST evaluations.

The 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. Should an officer initiate enforcement action against a person, motivated even in part by a person's actual or perceived race, color, ethnicity, or national origin, that enforcement action violates NYPD policy unless the officer's decision is based on a specific and reliable suspect description that includes not only race, age, and gender, but other identifying characteristics or information.