The City of New York
Department of Investigation

JOCELYN E. STRAUBER
COMMISSIONER

180 MAIDEN LANE
NEW YORK, NY 10038
212-825-5900

Release #25-2024
nyc.gov/doi

FOR IMMEDIATE RELEASE
THURSDAY, MAY 30, 2024

CONTACT: DIANE STRUZZI
(212) 825-5931

DOI'S OFFICE OF THE INSPECTOR GENERAL FOR THE NYPD (OIG-NYPD) ISSUES REPORT ASSESSING NYPD'S COMPLIANCE WITH THE PUBLIC OVERSIGHT OF SURVEILLANCE TECHNOLOGY (POST) ACT

The Department of Investigation's ("DOI") Office of the Inspector General for the New York City Police Department ("OIG-NYPD") released today its second Report concerning the New York City Police Department's compliance with the Public Oversight of Surveillance Technology ("POST") Act. OIG-NYPD reviewed the NYPD's Impact and Use policies, required by the POST Act, applicable to five surveillance technologies NYPD introduced in Calendar Year 2023: (1) Digidog, a remotely-operated robot; (2) the Knightscope K5 Autonomous Security Robot ("K5"); (3) StarChase GPS tracking technology ("StarChase"), which allows officers to attach GPS trackers to moving vehicles; (4) IDEMIA Mobile Biometric Check application ("IDEMIA"), a smartphone application capable of collecting and comparing digital fingerprints; and (5) an augmented reality smartphone application ("the AR application"), built by NYPD's Information Technology Bureau, capable of displaying data from NYPD databases concerning a particular location, when a smartphone camera is pointed at that location. Based on its review, OIG-NYPD made a number of findings and issued seven recommendations. A copy of OIG-NYPD's Report is attached to this release and can be found here: https://www.nyc.gov/site/doi/oignypd/web/report.page

DOI Commissioner Jocelyn E. Strauber said, "Surveillance technology is both a critical law enforcement tool as well as a matter of significant public concern. In New York City, the POST Act plays an important role in increasing public transparency with respect to the NYPD's use of surveillance technologies. This Report reiterates a significant finding from our 2022 analysis — that grouping surveillance technologies within a single Impact and Use Policy ("IUP") can limit the public transparency that the POST Act seeks to ensure, and makes other recommendations concerning the content of the IUPs."

Inspector General Jeanene L. Barrett said, "Monitoring NYPD's Impact and Use policies applicable to surveillance technologies is essential for instilling public confidence that these sophisticated technologies will be used responsibly. The recommendations in this Report will enhance these policies, increase transparency, and facilitate future oversight."

The POST Act requires that NYPD publicly propose an Impact and Use Policy at least 90 days prior to the use of any new surveillance technology. The public then has 45 days to submit comments on the proposed IUP to NYPD's Commissioner, who is then required to consider the public comments and publish a final IUP within 45 days of the close of the public comment period. When NYPD seeks to acquire or acquires enhancements to existing surveillance technology or uses such technology for a purpose or in a manner not previously disclosed in the IUP, the POST Act requires NYPD to provide an addendum to the existing IUP describing the enhancement or additional use. The POST Act further requires that DOI prepare annual audits of surveillance technology IUPs that: (1) assess NYPD's compliance with the terms of the applicable IUP; (2) describe any known or reasonably suspected violations of the IUP; and (3) publish recommendations, if any, relating to revisions of any IUP.

more

The 2023 announcement of NYPD's use of these technologies generated immediate concern from members of the public about the information the technologies could collect, access to the information, and the nature of the technologies' full capabilities. Members of the public also criticized NYPD for not complying with the POST Act based on the theory that these technologies required new IUPs.

OIG-NYPD's review found that NYPD did not issue any new IUPs in conjunction with the deployment of any of these five surveillance technologies. NYPD did; however, issue five addenda to existing IUPs in April 2023 purporting to cover NYPD's usage of K5, StarChase, IDEMIA, and the AR application. According to NYPD, the new Digidogs did not call for an addendum because the technology was already addressed in an existing IUP.

Based on its review, OIG-NYPD concludes that NYPD continues to group distinct surveillance technologies within a single IUP, a practice discussed extensively in OIG-NYPD's first annual report pursuant to the POST Act, which was released in November 2022. That review found that this grouping approach poses a risk that individual technologies could be shielded from public scrutiny and oversight. It was, and continues to be OIG-NYPD's position that the POST Act requires an IUP for each distinct surveillance technology, except in the limited circumstance where the surveillance technologies being grouped are substantially similar in capability and manner of use, and the IUP identifies and specifically names the individual technologies to which the IUP applies.

This review evaluates whether NYPD complied with the POST Act with respect to its use of the five above-referenced technologies and the sufficiency of the applicable IUPs. Based on its review, OIG-NYPD made the following findings:

1) NYPD has used grouping in an overly expansive manner by continuing to include Digidog within the existing Situational Awareness Cameras' ("SAC") IUP, rather than issuing an individual IUP, effectively undermining goals of the POST Act and limiting public transparency with respect to Digidog.

2) NYPD's grouping approach creates a risk that individual technologies may be shielded from public scrutiny and oversight, limiting the transparency about these technologies that the POST Act sought to create.

3) OIG-NYPD continues to maintain, as it did in its 2022 POST Act report, that Digidog was a surveillance technology with distinct capabilities and should have had a separate IUP when it was deployed in 2021. The new Digidogs purchased and deployed in 2023 include enhancements to the prior Digidog, which should have, at a minimum, been addressed in an addendum to the SAC IUP, since there was no separate IUP for Digidog.

4) K5, StarChase, IDEMIA, and the AR application were appropriately identified as enhancements to or new uses of existing surveillance technology, and therefore, the issuance of an addendum for each technology was appropriate under the POST Act.

5) Nevertheless, while K5, StarChase, IDEMIA, and the AR application were appropriately introduced via addenda in existing IUPs, the IUPs are insufficient because they do not include all of the information required by the POST Act:

    a. The SAC IUP does not disclose health and safety information with respect to K5;
    b. The GPS Tracking Devices IUP does not adequately disclose the specialized rules, processes, and guidelines that distinguish StarChase technology from other GPS tracking technologies, health and safety information, or the type of data that may be disclosed to external entities;
    c. Neither the Digital Fingerprint Scanning Devices IUP nor the Personal Electronic Devices' IUP provide sufficient information about IDEMIA with respect to policies and procedures related to data retention and access;
    d. The Portable Electronic Devices' IUP does not provide sufficient information about the AR application regarding policies and procedures related to data retention and access.

The review made the following seven recommendations based on OIG-NYPD's findings:

1. NYPD should issue a new individual IUP for Digidog.

2. NYPD should amend the addenda to the IUPs applicable to StarChase, IDEMIA, and the AR application to meet all of the requirements of the POST Act. The GPS Tracking Devices IUP should be updated to adequately disclose the specialized rules, processes, and guidelines, health and safety impacts, and the type of data that may be shared with external entities in relation to StarChase; the Digital Fingerprint Scanning Devices IUP should be updated to adequately address policies and procedures related to data retention and access in relation to IDEMIA; and the Portable Electronic Devices IUP should be updated to adequately disclose policies and procedures regarding data retention and access in relation to the AR application.

3. In the event that NYPD uses K5 in the future, the Department should disclose health and safety information related to the technology within the SAC IUP.

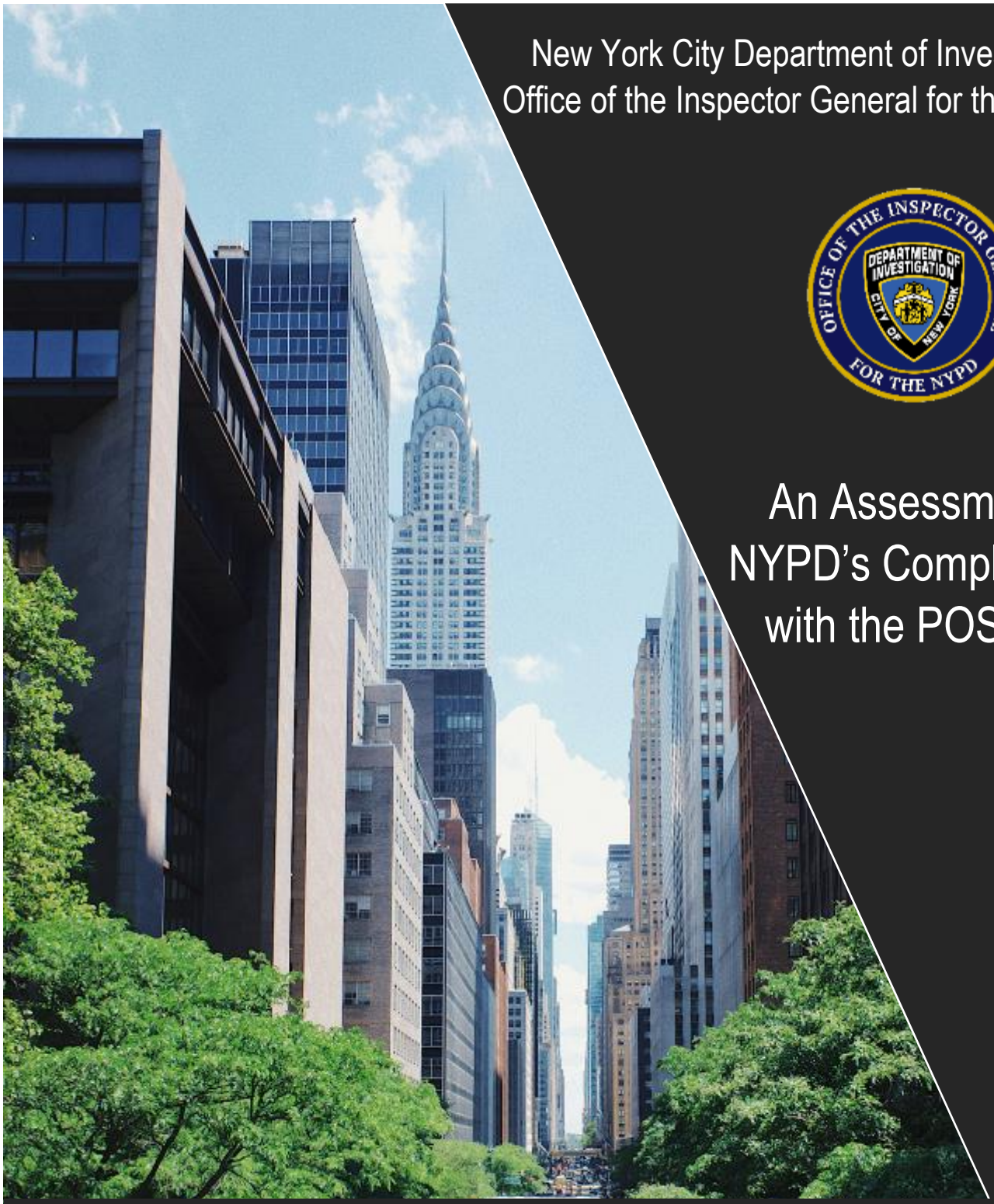
4. For future IUPs, NYPD should group surveillance technologies into single IUPs only when the surveillance technologies at issue are substantially similar in capability and manner of use, and the IUP identifies and specifically names the individual technologies to which specific information within the IUP applies.

5. NYPD should review its existing IUPs that "group" multiple surveillance technologies to determine if grouping is permissible under the standard set out in Recommendation 4, and issue new IUPs or addenda as appropriate.

6. While not a requirement of the POST Act, NYPD should update the Internal Audit and Oversight sections of its IUPs to include mechanisms for tracking and monitoring use of its surveillance technologies to ensure that the technologies are being used as described in the IUPs, and that the IUPs do not result in a disparate impact on any protected groups.

7. OIG-NYPD continues to maintain, as it did in its 2022 Report, that while not a requirement of the POST Act, NYPD should include in each IUP the potential disparate impacts of the surveillance technology on protected groups (instead of the potential disparate impacts of the IUP on protected groups, as is currently required under the law).

This review was prepared by DOI's Office of the Inspector General for the NYPD, specifically, Senior Investigative Policy Analyst McKenzie Dean under the guidance of Inspector General Jeanene L. Barrett with the assistance of Investigative Policy Analyst Olivia Sykes and First Deputy Inspector General Annette B. Almazan, and was supervised by Deputy Commissioner of Strategic Initiatives Christopher Ryan and Deputy Commissioner/Chief of Investigations Dominick Zarrella.



New York City Department of Investigation
Office of the Inspector General for the NYPD

An Assessment of NYPD's Compliance with the POST Act

May 2024

Jocelyn E. Strauber
Commissioner

Jeanene L. Barrett
Inspector General

I. Executive Summary

In 2020, New York City enacted the Public Oversight of Surveillance Technology ("POST") Act, which requires that the New York City Police Department ("NYPD" or "the Department") publicly disclose information concerning its use of surveillance technologies and its policies with respect to those technologies. Specifically, the POST Act requires that the Department publicly propose an Impact and Use Policy ("IUP") at least 90 days prior to the use of any new surveillance technology.[1] The public then has 45 days to submit comments on the proposed IUP to NYPD's Commissioner, who is then required to consider the public comments and publish a final IUP within 45 days of the close of the public comment period.[2] When NYPD seeks to acquire or acquires enhancements to existing surveillance technology, or uses existing surveillance technology for a purpose or in a manner not previously disclosed in the IUP, the POST Act requires NYPD to provide an addendum to the existing IUP describing the enhancement or additional use.[3]

The POST Act further requires that the New York City Department of Investigation ("DOI") prepare annual audits of surveillance technology IUPs that: (1) assess NYPD's compliance with the applicable IUP for that technology; (2) describe any known or reasonably suspected violations of the IUP; and (3) publish recommendations, if any, relating to revisions of any IUP.[4]

This year's annual report, issued by DOI through its Office of the Inspector General for the NYPD ("OIG-NYPD" or "the Office"), focuses on five policing technologies introduced by NYPD in calendar year 2023. On April 11, 2023, NYPD announced the use of three of these "new policing technologies" during a citywide press conference—remotely-operated robot dogs called Digidogs, the Knightscope K5 Autonomous Security Robot ("K5"), and StarChase GPS tracking technology ("StarChase"), which

* DOI Commissioner Jocelyn E. Strauber and Inspector General Jeanene L. Barrett thank the staff of OIG-NYPD for their efforts in producing this Report, specifically, McKenzie Dean, Senior Investigative Policy Analyst and Olivia Sykes, Investigative Policy Analyst. Appreciation is extended to the New York City Police Department and representatives of other organizations for their assistance and cooperation during this investigation.

[1] *See* N.Y.C. ADMIN. CODE § 14-188(b).
[2] *See* N.Y.C. ADMIN. CODE §§ 14-188(e) and (f).
[3] *See* N.Y.C. ADMIN. CODE § 14-188(d).
[4] *See* N.Y.C. CHARTER § 803(c-1).

can attach GPS trackers onto moving vehicles for real-time GPS tracking.[5] NYPD purchased two new Digidogs for deployment following a 2021 pilot program, using a prior version of the Digidog, which was discontinued by then-Mayor de Blasio.[6] K5 and StarChase were deployed as new pilot programs.[7] While not addressed at the press conference, the Department also introduced two new smartphone applications in 2023—the IDEMIA Mobile Biometric Check application ("IDEMIA"), capable of collecting and comparing digital fingerprints, and an augmented reality application ("the AR application"), built by NYPD's Information Technology Bureau, capable of displaying data associated with particular locations that is stored within NYPD databases. The K5 pilot program was completed in February of 2024, and the Department thereafter retired the robot.[8] It is OIG-NYPD's understanding that the other four technologies remain in use as of the date of this report.

NYPD did not issue any new IUPs in conjunction with the deployment of any of these surveillance technologies. It did, however, issue five addenda on April 11, 2023 to existing IUPs, specifically the IUPs for Situational Awareness Cameras ("SAC"), Global Positioning System ("GPS") Tracking Devices, Portable Electronic Devices ("PED"), Digital Fingerprint Scanning Devices, and Thermographic Cameras. The addenda stated that they applied to NYPD's usage of K5, StarChase, IDEMIA, and the AR application. Two additional addenda were issued on December 7, 2023, one to the Situational Awareness Cameras and one to the Portable Electronic Devices IUPs, related to K5 and IDEMIA, respectively. According to NYPD, no addendum was required to cover the new Digidogs because Digidog was already covered by the existing Situational Awareness Cameras IUP, issued in 2021, before the first deployment of Digidog.

The April 11, 2023 announcement generated immediate concern from members of the public about what information the technologies would collect, who would have access

---

[5] *See* N.Y.C. Mayor's Office, *Transcript of "Mayor Adams Makes Public Safety Announcement With NYPD Commissioner Sewell"* (Apr. 11, 2023), *at* https://www.nyc.gov/office-of-the-mayor/news/246-23/transcript-mayor-adams-makes-public-safety-announcementnypd-commissioner-sewell (last accessed Mar. 20, 2024).

[6] *See* Mihir Zaveri, *N.Y.P.D. Robot Dog's Run Is Cut Short After Fierce Backlash*, N.Y. TIMES, Apr. 28, 2021, *at* https://www.nytimes.com/2021/04/28/nyregion/nypd-robot-dog-backlash.html (last accessed Mar., 21, 2024) and N.Y.C. Police Dep't, *Spot Purchase Package records* (Jan.18, 2023). The first version of Digidog was retired in April 2021.

[7] *See* N.Y.C. Mayor's Office, *supra* note 5.

[8] *See* Dana Rubinstein and Hurubie Meko, *Goodbye for Now to the Robot That (Sort Of) Patrolled New York's Subway*, N.Y. TIMES, Feb. 2, 2024, *at* https://www.nytimes.com/2024/02/02/nyregion/nypd-subway-robot-retires.html (last accessed Mar. 20, 2024).

to the information, and the nature of the technologies' full capabilities. Some members of the public also criticized NYPD for not complying with the POST Act with respect to the surveillance technologies, based on the theory that these technologies required new IUPs, which NYPD did not issue.[9] On June 8, 2023, The Legal Aid Society filed a complaint with OIG-NYPD alleging that the addenda to existing IUPs were insufficient under the POST Act and that new IUPs should have been proposed with an opportunity for public comment because the surveillance technologies announced in April were "new and differ in impact and use to other surveillance tools already in use by the NYPD."[10]

The focus of this criticism, therefore, relates to NYPD's continued practice of grouping multiple surveillance technologies into single IUPs, a practice discussed extensively in OIG-NYPD's first annual report pursuant to the POST Act, which was released in November 2022. Grouping refers to the practice of issuing a single IUP to cover several surveillance technologies that are similar and have some overlapping capabilities. In the first annual report, OIG-NYPD found that this grouping approach poses a risk that individual technologies could be shielded from public scrutiny and oversight. It was, and continues to be, this Office's position that the most logical reading of the POST Act's language is that it requires an IUP for each surveillance technology, except in the limited circumstance where the surveillance technologies being grouped are substantially similar in capability and manner of use, and the IUP identifies and specifically names the individual technologies to which specific information within the IUP applies.

This report evaluates whether NYPD complied with the POST Act regarding its deployment of the five above-referenced technologies, and determines whether the manner in which NYPD addressed the new surveillance technologies in its IUPs was sufficient under the law. To perform its review, OIG-NYPD requested and reviewed all records provided by NYPD concerning the five technologies, including all policies, procedures, training material, and deployment documentation. OIG-NYPD also conducted a section-by-section review of the existing IUPs and addenda NYPD

[9] *See* Dana Rubinstein, *Security Robots. DigiDog. GPS Launchers. Welcome to New York*, N.Y. TIMES, Apr. 11, 2023, *at* https://www.nytimes.com/2023/04/11/nyregion/nypd-digidog-robot-crime.html (last accessed Mar. 21, 2024); *see also* Annie McDonough, *NYPD may be violating police surveillance transparency law*, CITY & STATE N.Y., Apr. 13, 2023, *at* https://www.cityandstateny.com/policy/2023/04/nypd-may-be-violating-police-surveillance-transparency-law/385173/ (last accessed Mar. 21, 2024).

[10] *See* Letter from Shane Ferro, The Legal Aid Society, to Jeanene Barrett, then-Acting Inspector General, OIG-NYPD (Jun. 8, 2023), *at* https://legalaidnyc.org/wp-content/uploads/2023/06/POST-Act-Letter-to-OIG-2023.pdf (last accessed Mar. 21, 2024).

identified as being applicable to Digidog, K5, StarChase, IDEMIA, and the AR application.

Based on its review, OIG-NYPD makes the following findings:

1) NYPD has used grouping in an overly expansive manner by continuing to include Digidog within the existing Situational Awareness Cameras' ("SAC") IUP, rather than issuing an individual IUP, effectively undermining goals of the POST Act and limiting public transparency with respect to Digidog.

2) NYPD's grouping approach creates a risk that individual technologies may be shielded from public scrutiny and oversight, limiting the transparency about these technologies that the POST Act sought to create. To the extent that grouped technologies are unique, this approach deprives members of the public of an opportunity for notice and comment with respect to the applicable IUP, and makes it more difficult for the public to discern the capabilities and use of the technologies and the policies applicable to them.

3) OIG-NYPD continues to maintain, as it did in its 2022 POST Act report, that Digidog is a surveillance technology with distinct capabilities and should have had a separate IUP when it was deployed in 2021. The new Digidogs purchased and deployed in 2023 include enhancements to the prior Digidog, which should have, at a minimum, been addressed in an addendum to the SAC IUP, since there was no separate IUP for Digidog.

4) K5, StarChase, IDEMIA, and the AR application were appropriately identified as enhancements to or new uses of existing surveillance technologies, and therefore, the issuance of an addendum for each technology was sufficient under the POST Act.

5) Nevertheless, while K5, StarChase, IDEMIA, and the AR application were appropriately introduced via addenda in existing IUPs, the IUPs are insufficient because they do not include all of the information required by the POST Act:
    a. The SAC IUP does not disclose health and safety information with respect to K5;
    b. The GPS Tracking Devices' IUP does not adequately disclose the specialized rules, processes, and guidelines that distinguish StarChase technology from other GPS tracking technologies, health and safety information, or the type of data that may be disclosed to external entities;

c. Neither the Digital Fingerprint Scanning Devices' IUP nor the Personal Electronic Devices' IUP provide sufficient information about IDEMIA with respect to policies and procedures related to data retention and access;
d. The Portable Electronic Devices' IUP does not provide sufficient information about the AR application regarding policies and procedures related to data retention and access.

II. Recommendations

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

1) NYPD should issue a new individual IUP for Digidog.

2) NYPD should amend the addenda to the IUPs applicable to StarChase, IDEMIA, and the AR application to meet all of the requirements of the POST Act. The GPS Tracking Devices' IUP should be updated to adequately disclose the specialized rules, processes, and guidelines, health and safety impacts, and the type of data that may be shared with external entities in relation to StarChase; the Digital Fingerprint Scanning Devices' IUP should be updated to adequately address policies and procedures related to data retention and access in relation to IDEMIA; and the Portable Electronic Devices' IUP should be updated to adequately disclose policies and procedures regarding data retention and access in relation to the AR application.

3) In the event that NYPD uses K5 in the future, the Department should disclose health and safety information related to the technology within the SAC IUP.

4) For future IUPs, NYPD should group surveillance technologies into single IUPs only when the surveillance technologies at issue are substantially similar in capability and manner of use, and the IUP identifies and specifically names the individual technologies to which specific information within the IUP applies.

5) NYPD should review its existing IUPs, that "group" multiple surveillance technologies to determine if grouping is permissible under the standard set out in Recommendation 4, and issue new IUPs or addenda as appropriate.

6) While not a requirement of the POST Act, NYPD should update the Internal Audit and Oversight sections of its IUPs to include mechanisms for tracking and monitoring use of its surveillance technologies to ensure that the

technologies are being used as described in the IUPs, and that the IUPs do not result in a disparate impact on any protected groups.

7) OIG-NYPD continues to maintain, as it did in its 2022 Report, that while not a requirement of the POST Act, NYPD should include in each IUP the potential disparate impacts of the surveillance technology on protected groups (instead of the potential disparate impacts of the IUP on protected groups, as is currently required under the law).

III. Background

A. The Public Oversight of Surveillance Technology ("POST") Act

Local Law 65 of 2020, commonly known as the POST Act, amended the Administrative Code of the City of New York to require the New York City Police Department ("NYPD" or "the Department") to publicly disclose information concerning its use of surveillance technologies and its policies with respect to those technologies.[11] Ninety days before using a new surveillance technology, NYPD must publicly post its proposed Impact and Use Policy ("IUP") for that technology. The public then has 45 days to comment on the proposed IUP, and the Department's Commissioner must consider those comments.[12] When NYPD seeks to acquire or acquires enhancements to existing surveillance technology, or to use such technology for a new purpose or manner, the Department must publish an addendum to the IUP for that technology; no public comment is required.[13]

The law 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]."[14] 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."[15]

[11] *See* Appendix A.
[12] *See* N.Y.C. ADMIN. CODE §§ 14-188(b), (e), & (f).
[13] *See* N.Y.C. ADMIN. CODE § 14-188(d).
[14] *See* N.Y.C. ADMIN. CODE § 14-188(a).
[15] *Id.*

The POST Act requires that for "the use of any new surveillance technology"[16] and "[f]or existing surveillance technology as of the effective date of the local law,"[17] NYPD must publish an IUP that includes the following information:

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

2) rules, processes, and guidelines issued by NYPD regulating access to or use of such surveillance technology as well as any prohibitions or restrictions on use;

3) safeguards or security measures designed to protect information collected by such surveillance technology from unauthorized access;

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 the type of entity, the type of information and data that may be disclosed, and any safeguards or restrictions imposed by NYPD regarding the use or dissemination of the information collected by such surveillance technology;

7) whether any training is required by NYPD 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 to ensure compliance with the IUP;

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

[16] *See* N.Y.C. ADMIN. CODE § 14-188(b).
[17] *See* N.Y.C. ADMIN. CODE § 14-188(c).

10) any potentially disparate impacts of the surveillance technology IUP on any protected groups as defined by the City's Human Rights Law.[18]

The POST Act also amended the New York City Charter to require that the New York City Department of Investigation ("DOI") prepare annual audits of surveillance technology IUPs that: (1) assess NYPD's compliance with the terms of the applicable IUP; (2) describe any known or reasonably suspected violations of the IUP; and (3) publish recommendations, if any, relating to revisions of any IUP.[19]

In November 2022, DOI's Office of the Inspector General for the NYPD ("OIG-NYPD" or "the Office") issued its first annual report pursuant to the POST Act.[20] This Office's investigation determined that NYPD largely complied with the POST Act's requirements with respect to the issuance of IUPs. However, OIG-NYPD also found that the IUPs did not contain sufficient detail to allow the Office to conduct a complete annual audit or to provide full transparency to the public. In particular, OIG-NYPD found that the IUPs contain, in part, boilerplate language that fails to provide sufficiently specific information about the nature of the technologies, the retention period for data obtained via use of the technologies, and the entities with which the data can be shared. The Office also found that NYPD grouped certain related technologies and issued a single IUP for each group. OIG-NYPD found that this approach significantly limited the information made available to the public concerning the nature and use of individual technologies (to the extent technologies within the group differ as to capability and function), and impeded the Office's ability to conduct meaningful oversight. As a result of the investigation, OIG-NYPD made 15 policy and procedure recommendations to NYPD, 14 of which NYPD subsequently rejected.

B. Deployment of Five Surveillance Technologies

On April 11, 2023, NYPD announced the use of three "new policing technologies" during a citywide press conference—remotely-operated robotic "dogs" called Digidogs, the Knightscope K5 Autonomous Security Robot ("K5"), and StarChase GPS tracking

---

[18] *See* N.Y.C. ADMIN. CODE § 14-188(a). The POST Act required that IUPs for "existing surveillance technology as of the effective date of the local law" be published within 180 days. *See* N.Y.C. ADMIN. CODE § 14-188(c).

[19] *See* N.Y.C. CHARTER § 803(c-1).

[20] *See* N.Y.C. Dep't of Investigation, AN ASSESSMENT OF NYPD'S RESPONSE TO THE POST ACT (Nov. 2022), *at* https://www.nyc.gov/assets/doi/reports/pdf/2022/20PostActRelease_Rpt_11032022.pdf (last accessed Mar. 20, 2024).

technology ("StarChase"), which can attach GPS trackers onto moving vehicles for real-time GPS tracking.[21] Specifically, NYPD purchased two new Digidogs for deployment. NYPD deployed an earlier version of Digidog in a 2021 pilot that then-Mayor de Blasio chose not to continue.[22] K5 and StarChase were deployed as new pilot programs.[23] While not addressed at the press conference, the Department also introduced two new smartphone applications—the IDEMIA Mobile Biometric Check application ("IDEMIA"), capable of collecting and comparing digital fingerprints, and an augmented reality application ("the AR application"), built by NYPD's Information Technology Bureau and capable of displaying data stored within NYPD databases that is associated with particular locations. The K5 robot pilot program was completed in February of 2024 and the Department thereafter retired the robot.[24] The other four technologies remain in use as of the date of this Report.

NYPD did not issue any new IUPs in conjunction with the 2023 deployment of any of the surveillance technologies described above. The Department did issue five addenda on April 11, 2023 to existing IUPs, specifically the IUPs for Situational Awareness Cameras ("SAC"), Global Positioning System ("GPS") Tracking Devices, Portable Electronic Devices ("PED"), Digital Fingerprint Scanning Devices, and Thermographic Cameras. The five addenda issued did not correspond one-to-one to the five technologies introduced by the Department. These addenda were intended to address NYPD's usage of K5, StarChase, IDEMIA, and the AR application. Two additional addenda were issued on December 7, 2023, for the SAC and PED IUPs, related to K5 and IDEMIA. According to NYPD, no addendum was required to address the new Digidogs because the Digidog device was referenced in the existing SAC IUP that was issued in 2021 in advance of the first deployment of Digidog.

C. Grouping Technologies into Single IUPs

Beyond the language cited above which defines a surveillance technology, the POST Act does not give further guidance about how substantially similar technologies should be treated with respect to unique IUPs, or how different devices that employ arguably similar surveillance technologies should be addressed. Moreover, the POST Act does not clearly delineate when a surveillance technology is merely an enhancement to an existing technology, as opposed to when it is sufficiently altered

[21] *See* N.Y.C. Mayor's Office, *supra* note 5.
[22] *See* Zaveri, *supra* note 6. The first version of Digidog was retired in April 2021.
[23] *See* N.Y.C. Mayor's Office, *supra* note 5.
[24] *See* Rubinstein and Meko, *supra* note 8.

or distinct to constitute an entirely new technology. On these points, NYPD and OIG-NYPD hold different views.

As discussed in more detail in OIG-NYPD's first annual report, while NYPD asserted that there are published IUPs applicable to each of the Department's surveillance technologies as required by the POST Act, certain IUPs cover groups of similar technologies, as opposed to individual technologies.[25] NYPD believed that it was appropriate to group the technologies under a single IUP that described their general capabilities and use because of the similarity and overlap of some surveillance technologies. At a December 2023 hearing before the New York City Council, NYPD reiterated its position that:

> [w]ithin a given surveillance technology will be different types of equipment and models, various forms in which the surveillance technology may be deployed, and a range of uses for that surveillance technology. We have not done a separate IUP and comment period for each type of hardware that deploys a given surveillance technology. Such an approach is not required by the POST Act.[26]

OIG-NYPD's first annual report found that this grouping approach poses a risk that individual technologies could be shielded from public scrutiny and oversight. It was, and continues to be, this Office's position that the most logical reading of the POST Act's language is that it requires an IUP for each distinct surveillance technology.[27]

OIG-NYPD believes that grouping is permitted under the POST Act only in the limited circumstance when the surveillance technologies being grouped in a single IUP are substantially similar in capability and manner of use, and the IUP identifies and specifically names the individual technologies to which specific information within the IUP applies.

As such, OIG-NYPD agrees that a new hardware device employing an existing surveillance technology would not require the publication of a new IUP, inasmuch as

---

[25] *See* N.Y.C. Dep't of Investigation, *supra* note 20, at 35-36.
[26] *See* N.Y.C. Council, *Transcript of Joint Hearing of Committee on Public Safety and Committee on Technology* (Dec. 15, 2023), *at* https://legistar.council.nyc.gov/View.ashx?M=F&ID=12694288&GUID=04E847F0-6A5F-4432-9810-B1F4A5B98498 (last accessed Mar. 21, 2024), at 17.
[27] This reading also is supported by the language of the POST Act. It defines an IUP with reference to "a surveillance technology," the singular form of the noun, not "the surveillance technologies." 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* N.Y.C. ADMIN. CODE § 14-188(a).

all the technological capabilities of the new hardware device are sufficiently addressed in an existing IUP.

However, in this Office's view, and as set forth in detail below, NYPD has utilized grouping in an overly expansive manner by addressing Digidog within the existing SAC IUP, rather than issuing an individual IUP. While the Department appropriately identified and introduced, via addenda, the other four technologies as enhancements to or new uses of existing technologies, the addenda did not fully satisfy the disclosure requirements of the POST Act. Thus, NYPD's approach undermines the goals of the POST Act and the public's interest in transparency.

D. Scope and Methodology of OIG-NYPD's 2023 Assessment of NYPD's Compliance with the POST Act

To conduct this review, OIG-NYPD reviewed all 36 of NYPD's IUPs, with a particular focus on the addenda issued on April 11, 2023, that together purported to cover the five surveillance technologies. OIG-NYPD examined additional policies and procedures, as well as user agreements and NYPD's comprehensive surveillance technology list, to determine whether the Department's practice of grouping multiple surveillance technologies under a single IUP was appropriate. The Office monitored deployments of the five technologies and interviewed various NYPD officials regarding the Department's use of the technologies.

IV. An Analysis of the New Technologies and the Relevant IUPs

A. Digidog

When the Department first piloted Digidog in 2021, it faced public backlash. Members of the public described the surveillance technology as "emblematic of how overly aggressive the police can be when dealing with poor communities."[28] New Yorkers and elected officials expressed a more general concern that Digidog was a threat to civil liberties, and objected to the cost of its procurement.[29] Ultimately, the first version of Digidog was retired in April 2021 after the Mayor's Office determined that it was "creepy, alienating, and sends the wrong message to New Yorkers."[30]

---

[28] *See* Zaveri, *supra* note 6.
[29] *See* Sophie Bushwick, *The NYPD's Robot Dog Was a Really Bad Idea: Here's What Went Wrong*, SCI. AM. (May 7, 2021) *at* https://www.scientificamerican.com/article/the-nypds-robot-dog-was-a-really-bad-idea-heres-what-went-wrong/ (last accessed Apr. 16, 2024).
[30] *See* Rubinstein, *supra* note 9.

Digidog's use in law enforcement is relatively new. Digidog, referred to as 'Spot' in a trademark by the manufacturer Boston Dynamics, is a two-foot tall, roughly four-foot long, quadrupedal robot weighing approximately 70 pounds.[31] The device is agile, flexible, and capable of walking up and down stairs and handling difficult terrain. Digidog's "face" has several cameras and is piloted by an operator using a tablet device with raised joysticks and buttons.[32]

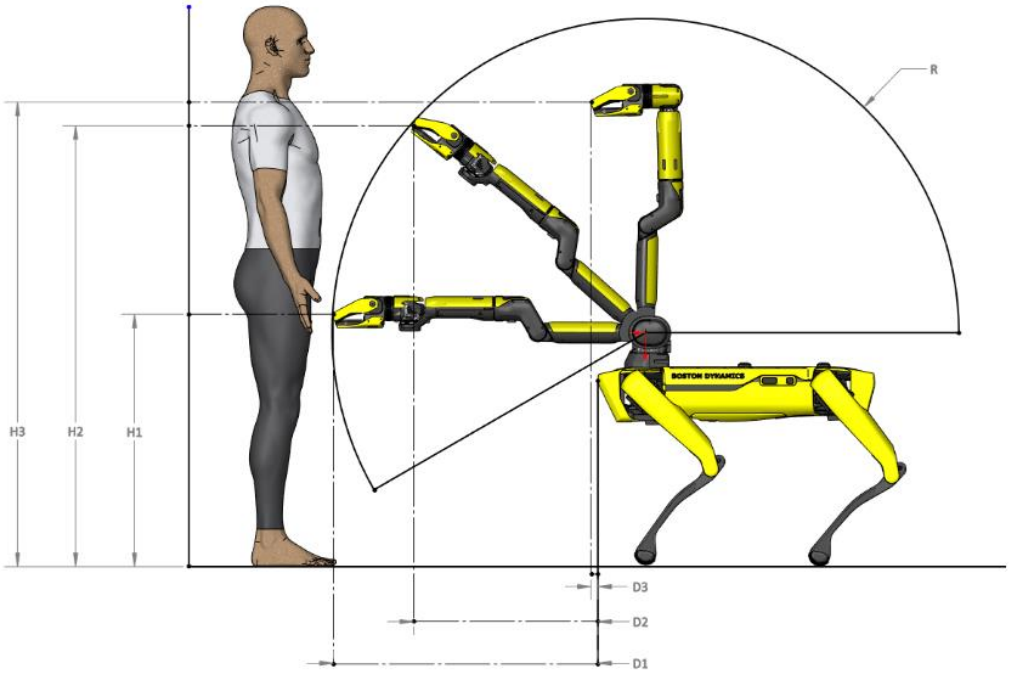


Figure 1: Basic Dimensions of Digidog with Spot Arm

According to NYPD, Digidog has been deployed five times in New York City. In 2023, Digidog was deployed twice—once by NYPD in July 2023 and once by the New York City Fire Department ("FDNY") in connection with the collapse of the Ann Street parking garage in Manhattan on April 18, 2023. The former version of Digidog was deployed on three occasions by NYPD in 2021.

NYPD continues to maintain that its current use of Digidog is covered by the original SAC IUP issued on April 11, 2021, despite OIG-NYPD's first POST Act report, which found that while that the SAC IUP referenced Digidog, it did not disclose to the public

[31] *See* Boston Dynamics, *Spot User Guide Release 2.0.1*, at 50.
[32] *Id.*, at 8.

the unique mobility capabilities, safety concerns, third-party ownership, and—while not a requirement of the POST Act—the potential disparate impacts associated with the Department's 2021 use of Digidog.

In light of the April 2023 announcement, OIG-NYPD probed whether there were any differences between the Digidog device used by the Department in 2021, and the Digidogs purchased in 2023. According to NYPD records, in 2021, the Department leased the Spot Explorer model of the Digidog.[33] However, NYPD records show that in 2023, the Department purchased two Spot Enterprise models of the Digidog.[34] In 2021, Boston Dynamics advertised the Explorer model as "the most basic package," compared to the Enterprise model, which included upgraded features of enhanced safety options, self-charging capabilities, and an unlimited Autowalk feature.[35] In 2023, Boston Dynamics' website did not differentiate between these two models, and referred to the device only as Spot, as its website does today.[36]

Based on OIG-NYPD's review of NYPD records, the Office determined that the two newly purchased Digidogs have additional technological capabilities or enhancements as compared to the model leased and used in 2021. These enhancements enable NYPD to use Digidog in manners not previously disclosed, such as to create 3D representations of its surroundings, collect information about the chemical composition of the atmosphere, manipulate objects and interact with the physical environment, and to take thermographic measurements.

Despite these technological enhancements, NYPD's April 11, 2023 addendum to the SAC IUP did not address these capabilities. OIG-NYPD continues to maintain that NYPD should have issued a separate IUP for Digidog prior to its 2021 use—rather than including it within the SAC IUP. Further, OIG-NYPD takes the position that the 2023 enhancements to the Digidogs should have been included in an addendum to what should have been a distinct IUP, but, at a minimum, the new Digidogs should have been addressed in an addendum to the existing Situational Awareness Cameras IUP that references Digidog. While the Department did issue an additional

[33] *See* N.Y.C. Police Dep't, *Agreement Between the City of New York Police Department and Boston Dynamics Inc.* (Sep. 23, 2020).
[34] *See* N.Y.C. Police Dep't, *Spot Purchase Package records* (Jan.18, 2023)
[35] *See* Boston Dynamics, *Spot*®, at https://web.archive.org/web/20210922214408/https://www.bostondynamics.com/spot (last accessed May 22, 2024).
[36] *See* Boston Dynamics, *Spot*®, at https://web.archive.org/web/20230118211302/https://bostondynamics.com/products/spot/#id_third and https://bostondynamics.com/products/spot/ (last accessed May 22, 2024).

addendum to the SAC IUP on December 7, 2023, that addendum, like the April 11, 2023 addendum, did not address Digidog.

Capabilities of the Technology

In 2023, NYPD acquired two new Digidog devices, both equipped with a thermal camera (SPOT Cam+ IR) and an arm attachment (Spot Arm). The Department also purchased one gas detection attachment to detect hazardous materials (Muve C360 Spot 8-Gas Detection Sensor) and an autonomous laser scanning attachment to create point cloud 3D representations of an environment (Leica BLK ARC Starter Pack).[37] It is unknown to the Office whether one of the Digidogs is equipped with both the gas detection and autonomous laser scanning attachments, or whether the two devices are equipped with one attachment each.[38]

The SAC IUP describes the general capabilities of situational awareness cameras as enabling NYPD "to observe inside barricaded, hazardous, or otherwise compromised locations from a safe location," allowing the Department to gather information about a location prior to physical entry.[39] It further states that one of the four types of situational awareness cameras used by NYPD includes cameras attached to remote controlled robots. The IUP states that "[s]elect situational awareness cameras, such as the NYPD 'Digidog' are capable of transmitting video images, acoustic data and enable two-way communication between NYPD personnel and any person near the device."[40]

OIG-NYPD finds this description of Digidog as a camera to be insufficient. Digidog is a robot that includes situational awareness cameras with capabilities that exceed those described in the SAC IUP. It is the Office's position that with respect to Digidog, a unique IUP addressing all of the technology's capabilities best serves public transparency and the goals of the POST Act.

---

[37] *See* N.Y.C. Police Dep't, *Spot Purchase Package records* (Jan.18, 2023).
[38] According to NYPD, as of the date of this report, the Digidog with hazardous materials detection capabilities has not yet been deployed.
[39] *See* N.Y.C. Police Dep't, *Situational Awareness Cameras IUP* (Dec. 7, 2023), at 3. *See also* N.Y.C. Police Dep't, *Situational Awareness Cameras IUP* (Apr. 11, 2021), at 3 and N.Y.C. Police Dep't, *Situational Awareness Cameras IUP* (Apr. 11, 2023), at 3. The most updated versions of the Department's IUPs can be found at https://www.nyc.gov/site/nypd/about/about-nypd/policy/post-act.page.
[40] *See* N.Y.C. Police Dep't, *Situational Awareness Cameras IUP* (Dec. 7, 2023), at 3. *See also* N.Y.C. Police Dep't, *Situational Awareness Cameras IUP* (Apr. 11, 2021), at 3 and N.Y.C. Police Dep't, *Situational Awareness Cameras IUP* (Apr. 11, 2023), at 3.

1. Spot Cam+ IR

The Spot Cam+ IR attachments equip both Digidog devices with a 360-degree camera with an integrated radiometric thermal camera, high-sensitivity microphones, and speakers.[41] Put another way, the Spot Cam+ IR allows NYPD to perform 360-degree surveillance using both standard and thermal cameras on each device, neither of which is disclosed in the SAC IUP in relation to Digidog.

The December 7, 2023 addendum to the SAC IUP discloses thermal measurement capabilities of K5, referred to in the IUP as the "autonomous security robot," thus seemingly acknowledging that such technology warrants an addendum to the IUP. However, the addendum does not reference Digidog, which has a similar capability. The addendum states:

> NYPD situational awareness cameras do not utilize video analytics, facial recognition, or any other biometric measuring technologies, *except to the extent that the autonomous security robot uses thermal imaging sensors to alert NYPD personnel of dangerously high temperatures and uses video-based sensors as part of its object avoidance system*" (emphasis added).[42]

2. Spot Arm Attachment

NYPD also purchased a semi-autonomous "Spot Arm" attachment for each of the Digidog devices in its possession. This modular add-on enables NYPD operators to utilize a distinct camera located at the end of the arm, which can be positioned to process video data at angles and of areas that other cameras on the device may be unable to reach.[43]

Additionally, the Spot Arm attachment allows the device to perform physical work, greatly extending Digidog's ability to interact with its environment.[44] The roughly

---

[41] *See* Boston Dynamics, *Spot CAM + IR*, *at* https://bostondynamics.com/wp-content/uploads/2020/10/spot-cam-plus-ir.pdf (last accessed Apr. 16, 2024).
[42] *See* N.Y.C. Police Dep't, *Situational Awareness Cameras IUP* (Dec. 7, 2023), at 3. OIG-NYPD notes that this statement is false as it relates to Digidog, which does in fact have biometric measuring technologies.
[43] *See* Boston Dynamics, *Impact people-centric environments with the Spot Arm*, *at* https://bostondynamics.com/products/spot/arm/ (last accessed Mar. 21, 2024).
[44] *Id.*

3.25-foot-long arm has a full range of motion and ends in a three-fingered gripper, with an embedded 4K camera, that is capable of lifting 11 kilograms (approximately 24.25 pounds) and dragging 25 kilograms (approximately 55.1 pounds).[45] The attachment enables the device to "[g]rasp, lift, carry, place, and drag a variety of items with the arm's 6-degrees of freedom and gripper," and "[s]emi-autonomously turn valves, flip levers, open doors, and manipulate other objects with constrained movement."[46] With this attachment, each Digidog is capable of examining suspicious backpacks or packages, looking around corners, and even opening doors, enabling the technology to process data that would otherwise be inaccessible to the device.

It is the Office's position that Digidog's ability to not only photograph objects readily within view, but to move and manipulate objects (at the direction of NYPD operators), and then photograph and obtain information about those objects (which is transmitted to NYPD operators), also brings the device within the definition of a surveillance technology, that is, "equipment, software, or systems capable of, used or designed for, collecting, retaining, processing, or sharing . . . video . . . location . . . or similar information, that is operated by or at the direction of [NYPD]."[47]

3. Leica BLK ARC Starter Pack

NYPD purchased a modular add-on for one of the two Digidog devices called the Leica BLK ARC Starter Pack. The BLK ARC is an "autonomous laser scanning module," which uses light detection and ranging technology to create point cloud 3D representations of an environment.[48] This information can then be used, in conjunction with the base camera, the Spot Cam+ IR, and the Spot Arm camera to better shape tactical or rescue operations. Despite equipping one of the two Digidog devices with an attachment that enables it to generate 3D images of its physical environment, this distinct technological capability is not mentioned in any of NYPD's updated IUPs.

4. Gas Detection Sensor

One of the two Digidogs acquired by the Department is capable of collecting information about the chemical composition of the atmosphere around the Digidog.

[45] *Id.*
[46] *Id.*
[47] *See* N.Y.C. ADMIN. CODE § 14-188(a).
[48] *See* N.Y.C. Police Dep't, *Spot Purchase Package records* (Jan.18, 2023).

NYPD acquired the MUVE C360 gas detector add-on, which attaches to the chassis of the device, and enables it to "provide real-time continuous monitoring of chemical hazards while on the move."[49] This distinct technological capability is not mentioned in any of NYPD's updated IUPs.

Rules, Processes, Guidelines, Restrictions, and Prohibitions for Use

As explained above, although the SAC IUP references the earlier version of Digidog, neither the original IUP, nor the April 11, 2023 or December 7, 2023 addenda, sufficiently addresses the rules and restrictions related to use of Digidog, and thus, do not satisfy the POST Act's requirement that these details be disclosed. As part of its investigation, OIG-NYPD reviewed a one-and-a-half-page NYPD Technical Assistance Response Unit ("TARU") Operational Guide and quick reference sheet outlining the procedures related to the deployment and basic operation of Digidog. The guide and the IUP appear to be inconsistent, which at a minimum, raises questions about the accuracy of the IUP with respect to the guidance, rules, and restrictions relating to the use of Digidog.

For example, the December 2023 SAC IUP states that "[u]se of Digidog can only be authorized by the Chief of Department."[50] However, TARU's Operational Guide makes no note of this requirement. The IUP also fails to disclose all of the general prohibitions and restrictions pertaining to the operation of Digidog technology, which are listed in the TARU Operational Guide as follows:

> *a. A Four-Legged Robot cannot be used for the following purposes:*
> *(1) Surveillance,*
> *(2) Routine Patrol, or*
> *(3) Immobilizing suspects or vehicles.*
> *b. A Four-Legged Robot will* ***not*** *be used as a weapon or equipped with any weapons.*
> *c. A Four-Legged Robot will* ***not*** *be equipped with facial recognition software.* (emphasis in original).[51]

The IUP does note that Digidog and other situational awareness cameras may not be equipped with facial recognition software and may not be used for routine foot patrol

---

[49] *See* Teledyne Flir, *MUVE™ C360, at* https://www.flir.com/products/muve-c360/?vertical=chem%20bio&segment=detection (last accessed Apr. 16, 2024).
[50] *See* N.Y.C. Police Dep't, *supra* note 42, at 4.
[51] *See* N.Y.C. Police Dep't, *TARU Operational Guide Number TARU-10, "Use of 4-Legged Robot (AKA Spot)"* (undated).

by officers, traffic enforcement, or immobilizing a vehicle or suspect, but the IUP does not prohibit the use of Digidog as a weapon or to be equipped with any weapons as is stated in TARU's guide. The NYPD's internal policies thus appear to be more restrictive in some respects than those described in the IUP, and less restrictive in other respects. Public disclosure of all applicable policies regarding the use of Digidog would further transparency and potentially reassure the public of the various controls NYPD has imposed on the use of Digidog.

Policies and Procedures Relating to Retention, Access, and Use of Data

The SAC IUP states that "[e]xcept for [K5], the NYPD does not record, store, or retain any of the video or acoustic data processed by situational awareness cameras."[52] The IUP does not address the storage of other types of data—such as infrared light data, point cloud data, and data regarding atmospheric conditions. Digidog can process all three types of data via the enhancements that the Department has acquired for it, namely the Spot Cam IR+, Leica BLK ARC, and the MUVE C360 gas detector, respectively. The SAC IUP as updated by addenda, thus, fails to fully address the policies and procedures relating to data retention with respect to Digidog.

External Entities

Because the SAC IUP does not address whether any of the non-video or acoustic data that Digidog can process is recorded, stored, or retained, it provides no information about whether such data is shared with external entities. Without this information, OIG-NYPD cannot properly assess whether the IUP or its addenda sufficiently addresses sharing Digidog data with external entities.

Internal Audit and Oversight Mechanisms

The SAC IUP fails to discuss any specific internal audit or oversight mechanisms related to Digidog for ensuring compliance with the IUP, and instead provides general information about who in NYPD has oversight responsibilities in relation to situational awareness cameras in general. The IUP notes that "[a] supervisor must periodically inspect and account for devices" and that "[s]upervisors of personnel utilizing situational awareness cameras are responsible for security and proper utilization of the technology and associated equipment."[53] Department

[52] *See* N.Y.C. Police Dep't, *supra* note 42, at 5. *See also* N.Y.C. Police Dep't, *Situational Awareness Cameras IUP* (Apr. 11, 2023), at 3.
[53] *See* N.Y.C. Police Dep't, *supra* note 42, at 5 and 9. *See also* N.Y.C. Police Dep't, *Situational Awareness Cameras IUP* (Apr. 11, 2023), at 4 and 8 and N.Y.C. Police Dep't, *Situational Awareness Cameras IUP* (Apr. 11, 2021), at 4 and 5.

representatives acknowledged to the Office that there are no written policies or mechanisms specific to Digidog that prevent its misuse or abuse. The Department relies instead on policies that broadly prevent misuse of all Department devices and systems, and those referenced in the SAC IUP (in which Digidog is included), which note the administrative and criminal penalties that may apply in the event of misuse of Department systems and data.

While Department representatives stated that Digidog is inspected twice a week by the TARU Response Team—to test the device's functionalities and ensure its batteries are charged—this procedure is not memorialized in a document or the IUP, nor are there any mechanisms to prevent misuse. While not required by the POST Act, in light of the expense and safety risks of Digidog, and the significant public concern about its use, the Department should establish internal audit and oversight mechanisms specifically related to Digidog surveillance technology and disclose those procedures in an IUP unique to Digidog.

Health and Safety Reporting

The SAC IUP uses the same boilerplate language that NYPD uses in the vast majority of its 36 IUPs. It states that "[t]here are no known health and safety issues with the use of situational awareness cameras or associated equipment."[54] However, with respect to Digidog, even a cursory reading of Boston Dynamic's User Guide identifies a number of safety concerns that should be disclosed pursuant to the POST Act's requirements as outlined below.[55]

a. Operational Safety Risks

The Boston Dynamics User Guide for Digidog states that "responsible use of [Digidog] is crucial to prevent dangerous conditions for operators and others nearby," and failure to use Digidog safely could lead to "serious injury [or] death."[56] In other

[54] *See* N.Y.C. Police Dep't, *supra* note 42, at 9. *See also* N.Y.C. Police Dep't, *Situational Awareness Cameras IUP* (Apr. 11, 2023), at 8 and N.Y.C. Police Dep't, *Situational Awareness Cameras IUP* (Apr. 11, 2021), at 5.
[55] *See* Boston Dynamics, *supra* note 31, at 9-13.
[56] *Id.*, at 9.

sections of both the Digidog and the Spot Arm User Guides, risks cited include broken bones, amputated fingers, pinched flesh, bruises, and death.[57]

Boston Dynamics further notes that

> [Digidog] is not suitable for tasks that require operation in close proximity to people. People must stay a safe distance (at least 2 meters [or over six-and-one-half feet]) from [Digidog] during operation to avoid injury. Injuries may be caused by collisions, [Digidog] falling or tipping onto people, or contact with [Digidog's] pinch points.[58]

Conditions that may cause Digidog to fall generally include stairs or inclines, signal loss, slippery surfaces, cords, and transparent or bright obstacles. The guide further notes that Digidog can collide with people or objects even while its obstacle detection is enabled, and anyone near the device should assume that it will move unexpectedly at any time.[59]

The manufacturer's guide to Digidog also includes a detailed discussion of tasks and environments not well-suited for Digidog. For example, Digidog should not be used "in home environments," "transporting hazardous materials or substances," "in potentially explosive environments," and "outside of controlled or restricted environment[s]."[60] The User Guide notes Digidog use in residential environments "may not provide adequate protection to radio reception in such environments."[61] It further states that Digidog is "suitable for areas where access is limited to trained

---

[57] *Id.*, at 9 (stating that "injuries may be caused by collisions, Spot falling or tipping onto people, or contact with Spot's pinch points…risk of serious injury, death"); at 10 (noting that "if Spot falls from an elevated position, it can cause serious injury or death"); at 12 (stating that "Spot's joints can pinch fingers and other body parts…Fingers may break or get amputated if caught in joints while Spot's motors are active"); at 13 (observing that there is a "risk of fire or electric shock"); and at 24 (commenting that "if Spot trips or is stopped it will fall down stairs and can injure anyone below it"). *See also* Boston Dynamics, *Spot + Spot Arm Information for Use (IFU) v1.0 Original Instructions* (2021), at 15 (referencing potential "[b]ruising…Tripping, dragging, and entanglement…cutting, puncturing… bone injury"), *at* https://d3cjkvgbik1jtv.cloudfront.net/Spot+IFU/spot_arm_information_for_use_EN_v1.0.pdf.

[58] *See* Boston Dynamics, *supra* note 31, at 9.

[59] *Id.*, at 10-11.

[60] *See* Boston Dynamics, *Spot + Spot Arm Information for Use (IFU) v1.0 Original Instructions* (2021), at 13-14.

[61] *See* Boston Dynamics, *supra* note 31, at 46.

personnel," and instructs the user to "keep untrained people away from [Digidog] during operation to avoid injury."[62]

Contrary to the restrictions outlined by Digidog's manufacturer, NYPD acknowledged deploying a Digidog device in July of 2023 inside a residential environment.[63] Since NYPD has failed to disclose any information related to Boston Dynamics' reports of health and safety effects related to Digidog, it is possible that the Department may have utilized the device in a manner inconsistent with its intended places of use.

Boston Dynamics also includes a warning on its website, which states, "[Digidog] as a stand-alone platform must be assessed for use in hazardous locations. For use in explosive environments, [Digidog] requires appropriate additional assessment and/or equipment."[64] The SAC IUP fails to address the safety assessments or additional equipment, if any, that have been conducted or supplied to prepare for Digidog's use in hazardous locations.

b. Battery Charging and Storage

FDNY has publicly warned New Yorkers of the dangers of lithium-ion batteries, which are a leading cause of fires and fire death in the City as of this year.[65] Lithium-ion batteries are also used for portable electronics such as electric bicycles or scooters. When this type of battery is not handled properly it can be extremely dangerous. According to FDNY, at least 113 lithium-ion battery-related fires have occurred in 2023, resulting in 71 injuries and 13 deaths.[66] FDNY explained that lithium-ion batteries "charged or stored incorrectly are very likely to overheat and catch fire—

[62] *Id.*, at 9.
[63] *See* N.Y.C. Council, *supra* note 26, at 83.
[64] *See* Boston Dynamics Support, *Spot Specifications*, *at* https://support.bostondynamics.com/s/article/Robot-specifications#Cameras (last accessed Apr. 16, 2024).
[65] *See* Fire Dep't of City of N.Y., *FDNY warns that lithium-ion batteries are now a leading cause of fires and fire deaths in New York City* (Feb. 2, 2024), *at* https://www.nyc.gov/site/fdny/news/Y40203/fdny-warns-lithium-ion-batteries-now-leading-cause-fires-fire-deaths-new-york (last accessed Apr. 16, 2024).
[66] *See* Robbie Sequeira, *Another Bronx building fire. A familiar cause: Lithium-ion batteries*, BRONX TIMES (Jun. 29, 2023), at https://www.bxtimes.com/bronx-building-fire-lithium-ion-batteries/ (last accessed Apr. 16, 2024).

which may cause battery cells to explode, resulting in rapidly-spreading, difficult-to-control fires."[67]

Yet, the SAC IUP indicates that there are no health and safety issues related to Digidog, despite being powered by a lithium-ion battery. Digidog's User Guide specifically contains a safety warning that the device's battery pack contains lithium, which is a highly reactive element that reacts violently when mixed with water and can lead to smoke and fire.[68]

As part of its safety plan, the Boston Dynamics User Guide directs that "[Digidog] operators should develop a battery storage and charging safety policy consistent with industry standards and local regulations."[69] The User Guide further provides specific instructions pertaining to battery safety to reduce the risk of fire or electric shock, which state that users should use only Boston Dynamics' provided batteries and chargers; refrain from disassembling or damaging its battery; remove the battery during transport and storage; and store, charge, and operate Digidog within specified temperature ranges. Further, in the event of a battery fire, users should refrain from attempting to extinguish the fire, and instead contact the fire department because battery fires create toxic fumes that cannot be put out conventionally.[70]

Despite the health and safety risks associated with lithium-ion batteries and the warnings provided by Digidog's manufacturer in relation to this equipment, NYPD has failed to disclose any information regarding these risks in the SAC IUP as required by the POST Act.

Disparate Impacts of the Impact and Use Policy

NYPD's SAC IUP technically complies with the POST Act, because the Act requires the IUP to address the disparate impact of the Impact and Use Policy itself, rather than the disparate impact of the surveillance technology on protected groups. As such, the Act does not require NYPD to publicly disclose any disparate impact related to the usage of Digidog, or any associated situational awareness cameras, on protected groups. However, OIG-NYPD takes the position that NYPD should nonetheless include in each IUP the potential disparate impacts of the use and

[67] *See* Kirstyn Brendlen and Lloyd Mitchell, *Lithium-ion batteries and e-bike catch fire in Bensonhurst building: FDNY*, BROOKLYN PAPER, https://www.brooklynpaper.com/lithium-ion-batteries-e-bike-fire-bensonhurst/ (last accessed Apr. 16, 2024).
[68] *See* Boston Dynamics, *supra* note 31, at 49.
[69] *Id.*, at 13.
[70] *Id.*

deployment of the surveillance technology itself on protected groups, as NYPD has done for certain, but not all, surveillance technologies.

B. The Knightscope K5 Autonomous Security Robot

Although NYPD's acquisition of K5 was announced at the April 2023 press conference, the pilot for its use did not begin until September 22, 2023, when it was deployed at the Times Square subway station.[71] At the press conference announcing the start of the pilot, Mayor Adams stated the following:

> The K5 will operate between midnight and six a.m. at the Times Square Subway Station for two months. With the duration of the trial, it will be accompanied by a police officer at all times, and for the first two weeks, it will be trained to map out the station, will move around the main station area and not on the platform… It will record video that can be viewed in case of an emergency or a crime. It will not record audio, and it will not use facial recognition. However, the K5 does have a button that connects you immediately to a live person that New Yorkers can utilize 24/7 with questions, concerns or to report an incident if needed.[72]

While NYPD described K5 as a "new policing technology" in April 2023, NYPD stated at a September 2023 press conference that "K5 is a robot that uses technology already in existence. We are taking an expensive camera network in the subway system and adding to it – supplementing to it, if you will – and adding a series of cameras that not only moves but a device that can connect subway riders to immediate assistance if the need arises."[73]

Like Digidog, the announcement of K5's use was met with some amount of public skepticism and concern. It was called "a trash can on wheels," "surveillance theater," and "an oversized version of R2-D2."[74]

---

[71] *See* Jeffrey C. Mays, *400-Pound N.Y.P.D. Robot Gets Tryout in Times Square Subway Station*, N.Y. TIMES (Sep. 22, 2023), at https://www.nytimes.com/2023/09/22/nyregion/police-robot-times-square-nyc.html (last accessed Mar. 22, 2024).
[72] *See* N.Y.C. Mayor's Office, *Transcript of "Mayor Adams Makes Public Safety-Related Announcement"* (Sep. 22, 2023), at https://www.nyc.gov/office-of-the-mayor/news/696-23/transcript-mayor-adams-makes-public-safety-related-announcement (last accessed Mar. 22, 2024).
[73] *Id.*
[74] *See* Mays, *supra* note 71.

K5's pilot program concluded in February 2024, and the robot was reportedly moved to an empty storefront in the Times Square Station.[75] The only record provided by the Department regarding the pilot program was the K5 Robot Deployment Plan, dated October 6, 2023. The plan described deployment of K5 in the Times Square subway station, patrolling a predefined route (following along a passageway between the 7th Avenue line and Times Square Tower) under the supervision of TARU personnel from 12:00 a.m. to 6:00 a.m.[76] The Office requested information related to the outcome of the K5 robot pilot program from NYPD, but, to date, has not received any responsive documents. While the Department remains in possession of K5, NYPD informed the Office that it has no plans to redeploy the technology now or in the future.

NYPD's surveillance technology inventory list indicates that K5 is addressed by the Closed-Circuit Television Systems and Thermographic Cameras IUP.[77] But OIG-NYPD's review of the Department's original IUPs and addenda reflects that, in fact, NYPD addressed K5's capabilities in the addenda to the SAC and the Thermographic Cameras IUPs and not the Closed-Circuit Televisions Systems IUP.

Capabilities of the Technology

K5 is a five-foot-two-inch-tall, 398-pound, fully autonomous weatherproof security robot capable of providing 24/7 patrol surveillance.[78] The device has the ability to navigate ADA compliant surfaces and ramps, travel up to a speed of three miles per hour, and autonomously recharge without human intervention.[79] K5 is equipped with four 360 degree HD cameras, one infrared camera, 16 microphones, and an amplified public announcement speaker.[80] The device enables live streaming to computers, tablets, and cell phones, it is equipped with 4G LTE Cellular connection, and it includes 30-days of raw video storage.[81]

---

[75] See Rubinstein and Meko, *supra* note 8.
[76] *See* N.Y.C. Police Dep't, *Internal Memorandum, "Transit Manhattan Task Force K5 Robot Deployment Plan"* (Oct. 6, 2023).
[77] *See* N.Y.C. Police Dep't, *POST Act Technology Inventory – All Units* (Apr. 25, 2024).
[78] *See* Knightscope, *K5 Outdoor/Indoor Use*, at https://assets.website-files.com/6261e4407c2b850439c5d724/63406292faa305184a3602c2_KI-brochure-K5-22Q3.pdf (last accessed Apr. 16, 2024).
[79] *Id.*
[80] *Id.*
[81] *Id.*

The SAC IUP, as amended by the April 11, 2023 and December 7, 2023 addenda, states generally that situational awareness cameras allow NYPD to "observe inside barricaded, hazardous, or otherwise compromised locations from a safe location" and allow personnel "to gather critical information about a queried location before entry."[82] Specific to autonomous security robots like K5, their use "will provide additional public safety resources and help deter crime."[83] Additionally, the IUP notes that the Department uses "[c]ameras attached to autonomous security robots travelling along pre-programmed routes."[84] The April 2023 addendum stated that K5 does not use video analytics or biometric measurement, but is capable of transmitting infrared thermal images, while the December 2023 addendum states that K5 does not use video analytics, facial recognition, or biometric measuring, except to the extent that it "uses thermal imaging sensors to alert NYPD personnel of dangerously high temperatures and uses video-based sensors as part of its object avoidance system."[85] While both the April 2023 and December 2023 versions of the SAC IUP sufficiently address the thermal measurement capabilities of K5, the April 2023 IUP inaccurately stated that K5 does not use biometric measurement. However, the December 2023 IUP appropriately acknowledges that K5's thermal measurement is a biometric measurement, and thus, sufficiently discloses the capabilities of K5.

The Thermographic Cameras IUP, as amended by the April 11, 2023 addendum, sufficiently addresses K5's capability of transmitting infrared thermal images, and appropriately discloses its thermal data retention period of 30 days. The document also refers readers to the SAC IUP for additional information.[86]

OIG-NYPD was unable to determine whether NYPD used K5 in accordance with the IUPs as NYPD provided no records related to the pilot program except for the deployment plan dated after the start of the pilot.

Rules, Processes, Guidelines, Restrictions, and Prohibitions for Use

As the Department did not produce any information regarding the policies or procedures related to K5's pilot program, aside from the deployment plan, OIG-NYPD was unable to fully assess whether NYPD followed the rules and guidelines included in its SAC or Thermographic Cameras IUPs, or whether these rules and guidelines

[82] *See* N.Y.C. Police Dep't, *supra* note 42, at 3. *See also* N.Y.C. Police Dep't, *Situational Awareness Cameras IUP* (Apr. 11, 2023), at 3.
[83] *Id.*
[84] *Id.*
[85] *See* N.Y.C. Police Dep't, *Situational Awareness Cameras IUP* (Apr. 11, 2023), at 3, 9 and N.Y.C. Police Dep't, *Situational Awareness Cameras IUP* (Dec. 7, 2023), at 3, respectively.
[86] *See* N.Y.C. Police Dep't, *Thermographic Cameras IUP* (Apr. 11, 2023), at 3.

were sufficiently disclosed within the IUPs. However, the SAC IUP was inconsistent with the Department's October 9, 2023 K5 Robot Deployment Plan. Although the SAC IUP states that a request for use of a situational awareness camera must be made to the Emergency Services Unit ("ESU") or TARU, and approved by a supervisor, K5 was deployed pursuant to a plan to utilize a regular, predefined route that, once approved by the Chief of Transit, did not require prior request or approval for daily use.

Policies and Procedures Relating to Retention, Access, and Use of Data

The SAC IUP accurately states that K5 retains video and acoustic data for 30 days, provides information related to policies associated with access to the data, and notes policies and procedures related to use of the collected data.[87]

Health and Safety Reporting

Both the SAC and Thermographic Cameras IUPs inaccurately claim that there are no known health or safety issues associated with the use of K5. In fact, there are general safety concerns associated with any type of robot autonomously navigating an area occupied by the public.

In 2016, a K5 patrolling a shopping center ran over and injured a 16-month-old child.[88] At the time of the incident, Knightscope's website claimed that the K5 robot could safely navigate around people and objects.[89] In 2017, a K5 patrolling a Washington, D.C. retail complex drove itself into a fountain after failing to detect a set of stairs. At the time of the incident, Knightscope's website claimed that its models "guide themselves through even the most complex environments."[90] While OIG-NYPD could not confirm that the K5 models involved in those incidents were the exact models procured by NYPD, these examples are illustrative of potential risks associated with having a 400-pound, five-foot-two-inch tall, fully autonomous device operating on a pre-programmed route in a high-traffic public area. Such risks are sufficient to warrant additional research and discussion in the IUP.

---

[87] *See* N.Y.C. Police Dep't, *supra* note 42, at 5. *See also* N.Y.C. Police Dep't, *Situational Awareness Cameras IUP* (Apr. 11, 2023), at 5.

[88] *See* Matt McFarland, *300-pound mall robot runs over* toddler, CNN BUSINESS, *at* https://money.cnn.com/2016/07/14/technology/robot-stanford-mall/index.html (last accessed Apr. 16, 2024).

[89] *Id.*

[90] *See* Christopher Mele, *Revealed: how the K5 security robot ended up in a fountain*, THE SYDNEY MORNING HERALD (Jul. 19, 2017), *at* https://www.smh.com.au/technology/revealed-how-the-k5-security-robot-ended-up-in-a-fountain-20170719-gxdz6s.html (last accessed Apr. 16, 2024).

Disparate Impacts of the Impact and Use Policy

NYPD's SAC and Thermographic Cameras IUPs technically comply with the POST Act, because the Act requires an IUP to address the disparate impact of the Impact and Use Policy itself, rather than the disparate impact of the surveillance technology on protected groups. As such, the Act does not require NYPD to publicly disclose any disparate impact related to the usage of K5, or any associated situational awareness and thermographic cameras, on protected groups. However, OIG-NYPD takes the position that NYPD should nonetheless include in each IUP the potential disparate impacts of the use and deployment of the surveillance technology itself on protected groups, as NYPD has done for certain, but not all, surveillance technologies.

C. StarChase GPS Tracking ("StarChase") Technology

StarChase is a surveillance technology that allows NYPD to attach a GPS tracker to a fleeing vehicle. According to NYPD, StarChase is covered by the GPS Tracking Devices IUP, as amended by the April 11, 2023 addendum, which notes that "GPS tracking devices used to track fleeing vehicles in limited circumstances will be tested by the NYPD for a 90-day period."[91] The IUP states that:

> [t]he use of GPS tracking devices allows NYPD personnel to obtain location data in situations where it is impractical or impossible to manually obtain that data through physical surveillance of a subject by NYPD personnel. Manual physical surveillance is resource intensive and inherently carries a risk that a subject may observe surveilling NYPD personnel and jeopardize the underlying investigation. GPS devices attached onto fleeing vehicles in limited circumstances will avoid vehicle pursuits and allow NYPD personnel to locate and track vehicles in a safer manner.[92]

At the April 2023 press conference, NYPD stated that the new StarChase technology had been deployed by officers responding to a report of a stolen vehicle the previous Saturday night, prior to the issuance of the addendum.[93] The target vehicle was

[91] *See* N.Y.C. Police Dep't, *Global Positioning System (GPS) Tracking Devices IUP* (Apr. 11, 2023), at 2.
[92] *Id.*, at 3.
[93] *See* Mayor's Office, *supra* note 5.

tagged using StarChase and followed into the Bronx, where it was pulled over. According to NYPD, the technology mitigated a pursuit, led to an arrest, and assisted NYPD with taking a stolen vehicle off the street.[94]

In response to a request for documentation related to StarChase deployments in 2023, the Office received 11 Vehicle Pursuit Reports. However, none concerned the incident referenced at the press conference. The Department instead provided internal correspondence in relation to the incident, which detailed a successful StarChase deployment that led to the apprehension of the perpetrator driving a stolen vehicle.

StarChase is distinct from other GPS tracking devices because it has mechanisms that allow it to attach a GPS device onto a fleeing vehicle. NYPD uses two forms of StarChase—a vehicle-mounted device (the Guardian-VX) and a handheld device (the Guardian-HX)—both of which have this capability.[95] While this use of a GPS tracking device is new, the Office found that the surveillance technology utilized by StarChase is identical to other GPS tracking technologies already used by NYPD. Therefore, OIG-NYPD agrees with NYPD's position that its use of StarChase only requires an addendum under the POST Act and not a new IUP.

However, OIG-NYPD found that the information contained in the GPS Tracking Devices IUP addendum was insufficient to satisfy other requirements of the POST Act. For example, StarChase is to be used on fleeing vehicles for the specific and limited purpose of "avoid[ing] vehicle pursuits and allow[ing] NYPD personnel to locate and track vehicles in a safer manner."[96] Unlike other GPS technology used by NYPD, a search warrant is not required to use StarChase. Based on this Office's review, use of this technology is governed by specialized rules, processes, and guidelines different from other GPS tracking technologies, which are not sufficiently disclosed within the IUP.

Capabilities of the Technology

The GPS Tracking Devices IUP describes the general capabilities of GPS tracking technology, which "identif[ies] or estimate[es] the geographic position of the tracking device" when "placed on a movable, physical object related to a subject of criminal

[94] *Id.*
[95] *Id.*

investigation."[97] The IUP also describes GPS tracking technology's ability to receive and process radio signals transmitted by GPS satellites and to generate coordinates associated with the location of the tracking device.[98]

While StarChase is distinct from other GPS tracking technologies because it can be placed, via a launch mechanism, onto a moving vehicle (that is, it can be placed without an individual being in close proximity to the vehicle and physically placing it on the vehicle), the surveillance technology capabilities are identical to those of the existing technologies covered by the IUP.

However, the IUP does not describe the mechanisms that allow StarChase to be used on a fleeing vehicle, specifically a vehicle-mounted device (the Guardian-VX) and a handheld device (the Guardian-HX)—both of which are capable of discharging a projectile onto a moving vehicle, for the purpose of mitigating high-speed pursuits.[99] The vehicle-mounted device deploys GPS tracking tags from a launcher that can be installed on the front of virtually any vehicle.[100] The handheld device is a single shot, air-powered launcher that serves as a portable alternative to the vehicle-mounted version of the technology.[101] According to StarChase, the hand-held Guardian-HX, operates at a velocity of 37 miles per hour and has a 35-foot range with an angled shot range of up to 60 feet.[102]

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

The GPS Tracking Devices IUP does not sufficiently disclose NYPD's rules and restrictions related to the use of StarChase surveillance technology. In addition to the IUP, OIG-NYPD reviewed an NYPD Operations Order, dated November 15, 2023, outlining the procedures related to the deployment and basic operation of StarChase. While the Operations Order and the IUP are largely consistent, the IUP is less specific than the Operations Order, which describes additional restrictions on the use of StarChase. This raises questions about the adequacy of the IUP, specifically with

[97] *Id.*
[98] *Id.*
[99] *See* Mayor's Office, *supra* note 5, at 3.
[100] *See* Starchase, *Guardian-VX Vehicle Mounted GPS Launcher*, *at* https://www.starchase.com/products/vehicle-mounted-gps-launcher/#features (last accessed Apr. 16, 2024).
[101] *See* Starchase, *Guardian-HX Hand-Held Launcher brochure*, *at* https://www.starchase.com/wp-content/uploads/2022/09/HHL-Tech-Sheet-for-Website-Download.pdf (last accessed Apr. 16, 2024).
[102] *Id.*

respect to its disclosure of the rules and restrictions relating to use, as required by the POST Act.

The IUP states that a GPS tracking device such as StarChase can be used without first obtaining a search warrant "when exigent circumstances exist and there is probable cause to believe that the vehicle was used in the commission of a crime or there is probable cause to believe that a person who is currently inside of the vehicle has committed a crime."[103] However, the November 2023 Operations Order appears to permit use of StarChase under narrower circumstances, only when there is probable cause that at least one of the following crimes has been committed:

1) Any crime where death has resulted (e.g., homicide, leaving the scene of a collision where a fatality occurs, etc.),
2) Robbery,
3) Burglary,
4) Felony Assault,
5) Criminal Possession of a Firearm,
6) Criminal Possession of a Weapon (felony),
7) Reckless Endangerment (i.e., involving a firearm or caused by manner in which individual is operating vehicle, etc.),
8) Reckless Driving where an individual has placed persons or property in danger and failed to, or refused to, comply with any lawful order or direction of any police officer, and/or
9) Any vehicle that has been reported stolen.[104]

Moreover, the IUP simply states that StarChase "will be used to track a vehicle from the time it [flees] until the vehicle and/or passengers can be safely recovered or apprehended,"[105] while the Operations Order details important legal considerations that govern the discontinuance of StarChase's use after deployment. Specifically, the Operations Order states that although StarChase technology may initially be deployed without a warrant in limited circumstances, these circumstances do not allow for the indefinite tracking of a vehicle. As a result, personnel must assess whether the tracking of a vehicle with the device may continue without a warrant if

[103] *See* N.Y.C. Police Dep't, *supra* note 91, at 4.
[104] *See* N.Y.C. Police Dep't, *Operations Order Number 49, Pilot Program – StarChase GPS Tracking System for Uniformed Members of the Service Assigned to the Patrol Services Bureau Community Response Team, Office of the Chief of Department, and Patrol Borough Queens South Public Safety Team* (Nov. 15, 2023).
[105] *See* N.Y.C. Police Dep't, *supra* note 91, at 4.

personnel cannot locate a tagged vehicle after a "reasonable amount of time."[106] The Operations Order explains that the factors that determine what constitutes a reasonable amount of time are "numerous and unique to each situation" and does not provide any additional information regarding this restriction.[107]

The Operations Order further describes several restrictions not disclosed within the GPS Tracking Devices IUP, specifically that:

1) Personnel should comply with the Department's Patrol Guide procedure 221-15 and not engage in vehicle pursuit solely for the purpose of deploying a StarChase device;
2) StarChase technology should not be deployed on any vehicle designed to be operated with fewer than four wheels, or that does not have an enclosed passenger compartment such as motorcycles, ATVs, and convertibles with the top down,
3) StarChase technology should not be used if conditions are unsafe, and
4) Deployment of StarChase technology from a handheld device must be done only by the recorder—or passenger—of the Department vehicle. (numbering added).[108]

The IUP merely states that StarChase will be used only by trained personnel to track a vehicle until "the vehicle and/or passengers can be safely recovered or apprehended."[109] Consistent with this Office's observations concerning the differences between the policies set out in the IUP and those contained in internal guidance with respect to Digidog, full disclosure of the NYPD's policies with respect to StarChase will provide additional transparency and potentially reassure the public with respect to the restrictions on the use of StarChase.

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

In reference to StarChase, the addendum to the GPS Tracking Devices IUP states that "access to the associated software is granted for the time period the device is in use. The location data for these devices will be retained for a period of three (3) years unless data has been identified to be retained for security purposes or for criminal investigations."[110]

---

[106] *See* N.Y.C. Police Dep't, *supra* note 104.
[107] *Id.*
[108] *Id.*, at 2, "Deployment of Starchase Device."
[109] *Id.*, at 3-4.
[110] *See* N.Y.C. Police Dep't, *supra* note 91, at 6.

External Entities

The GPS Tracking Devices IUP repeats the same boilerplate language used in each IUP with respect to information and data access in relation to outside entities. OIG-NYPD found that NYPD has a "sharing agreement" with a local law enforcement entity with respect to StarChase, which is not mentioned within the IUP—however, the IUP notes that government agencies at the local, state, and federal level have limited access to NYPD computer and case management systems subject to written agreements.[111] Therefore, the IUP sufficiently discloses whether entities outside NYPD have access to the data, appropriately acknowledges that this is inclusive of local agencies, and notes the safeguards imposed on such entities. However, the IUP does not note the type of information and data that may be disclosed to such entities as is required by the POST Act.

Internal Audit and Oversight Mechanisms

The GPS Tracking Devices IUP and its addendum focuses on audits of computer terminal activity, the role of supervisors in deciding whether the surveillance technology will be used, ensuring it is used within NYPD guidelines, and the role of Integrity Control Officers ("ICOs") in ensuring that personnel comply with computer security guidelines. There is no indication that NYPD is analyzing the use of StarChase, or any other GPS tracking technology, to assess the technology's use by officer, by frequency, by location or command, by the demographics of individuals in the vehicle, or any other quantitative or qualitative metrics. While monitoring and disclosure of this information would extend beyond the requirements of the POST Act, the Office recommends that NYPD develop mechanisms to closely examine the use of such technology to determine any areas for improvement, and include this information within the IUP.

Health and Safety Reporting

The GPS Tracking Devices IUP and its addendum state there are no known health and safety issues associated with GPS tracking devices. As with the previous surveillance technologies, this is inaccurate. The Department's Operations Order specifically contemplates possible injury during the deployment of StarChase and instructs officers to comply with NYPD's "Reporting and Investigation of Force Incident or Injury to Persons During Police Action" procedure if anyone sustains an

[111] *See* N.Y.C. Police Dep't, *supra* note 104, and N.Y.C. Police Dep't, *supra* note 91, at 3.

injury from being struck by StarChase equipment.[112] In fact, StarChase is classified as a use of force by its manufacturer, describing its handheld launcher as "less lethal," with a "non-lethal" rating and its vehicle-mounted launcher as having a "non-lethal" rating.[113]

According to the National Institute of Justice's overview of less-lethal technologies, even these technologies, while alternatives to other potentially more dangerous physical force options, still involve a use of physical force, and thus pose potential health and safety risks.[114] Other technologies grouped within this category along with StarChase technology include tasers, pepper spray, tear gas, and blunt force projectiles.[115]

While the principal purpose of StarChase technology is to avoid high-speed vehicle pursuits that pose significant health and safety risks to both officers and the community—and while there have been several successful deployments of the technology that have reportedly reduced such risks—the IUP is inaccurate in stating there are no known health and safety issues associated with StarChase equipment.[116] Accordingly, the IUP does not comply with the POST Act's requirement that health and safety effects of the surveillance technology be included in an IUP.

Disparate Impacts

NYPD's GPS Tracking Devices IUP technically complies with the POST Act, because the Act requires the IUP to address the disparate impacts of the Impact and Use Policy itself, rather than the disparate impact of the surveillance technology on protected groups. As such, the Act does not require NYPD to publicly disclose any disparate impact related to the usage of StarChase, or any associated GPS tracking devices, on protected groups. However, OIG-NYPD takes the position that NYPD should nonetheless include in each IUP the potential disparate impacts of the use and deployment of the surveillance technology itself on protected groups, as NYPD has done for certain, but not all, surveillance technologies.

---

[112] *See* N.Y.C. Police Dep't, *supra* note 104.
[113] *See* Starchase, *Guardian-HX Handheld GPS Launcher*, at https://www.starchase.com/products/handheld-gps-launcher/ (last accessed Apr. 16, 2024) and Starchase, *supra* note 97.
[114] *See* Nat'l Institute of Justice, *Overviews of Less-Lethal* Technologies (Jun. 11, 2011), *at* https://nij.ojp.gov/topics/articles/overview-less-lethal-technologies (last accessed Apr. 16, 2024).
[115] *Id.*
[116] *See* Nat'l Institute of Justice, *Technology for Pursuit Management* (Mar. 3, 2013), *at* https://nij.ojp.gov/topics/articles/technology-pursuit-management (last accessed Apr. 16, 2024).

D. IDEMIA Biometric Check Application

According to NYPD, the IUPs relevant to IDEMIA are the Digital Fingerprinting Scanning Device and the Portable Electronic Devices IUPs as amended by their respective April 11, 2023 addenda. Based on OIG-NYPD's review, it appears that the two IUPs sufficiently describe the capabilities and use of IDEMIA. However, OIG-NYPD also concluded that, in certain respects, the IUPs do not provide sufficient information regarding policies and procedures relating to data, as required by the POST Act.

Capabilities and Rules, Processes and Guidelines Relating to the Use of the Technology

The April 2023 addendum to the Digital Fingerprint Scanning Devices IUP appropriately describes the capabilities of IDEMIA as a distinct application from the other digital fingerprint scanning devices described in the IUP. IDEMIA, which is differentiated from stationary digital fingerprint scanners and is available on only "some NYPD-issued Personal Electronic Devices (PED)," allows for identification confirmation by a digital fingerprint scan. A small number of tablets have a peripheral device to conduct a digital fingerprint scan, which is transmitted for comparison in the same manner as the physical equipment."[117] The application enables officers to conduct touchless fingerprint scans using their smartphone camera in the field.[118] If the application detects a match, it returns information pertaining to the "matched" individual's identity, including any active warrants for that person.[119]

Unlike other Department fingerprint scanning devices, this application only compares the picture of an individual's fingerprints to data from NYPD's local Automated Fingerprint Identification System ("AFIS"), rather than to data from the local, state, and national AFIS systems.[120] NYPD's AFIS database contains known fingerprints (fingerprints associated with a particular individual) and evidence fingerprints (fingerprints collected from a crime scene or other relevant locations that are not associated with a particular individual).[121]

---

[117] *See* N.Y.C. Police Dep't, *Digital Fingerprint Scanning Devices IUP* (Apr. 11, 2023), at 4.
[118] *See* N.Y.C. Police Dep't, *Operations Order Number 61 – Use of the Idemia Morphio Biometric Check Application by Members of the Service* (Nov. 22, 2022).
[119] *See* N.Y.C. Police Dep't, *supra* note 117, at 4.
[120] *Id.*, at 5.
[121] *Id.*, at 4.

Select personnel assigned to the Criminal Justice, Detective, Housing, Patrol, and Transit Bureaus have been issued smartphones that provide access to the IDEMIA application and can be used by officers depending on their specific assignment.[122] Use of the application requires consent of the individual to be scanned, except in exigent circumstances, such as an encounter with an unknown individual with dementia.[123]

The Digital Fingerprint Scanning Devices IUP provides specific examples of the purposes for which the application may be used, which correspond to the assignments of personnel provided access to the technology:

a) to confirm the identity of a defendant appearing at arraignment. . . ,
b) to aid in the identification of deceased and/or unknown persons, and
c) to confirm the identity of a person for issuance of a summons in the field.[124]

The IUP provides limited information regarding (b) and, in particular, with respect to circumstances in which use of the application to identify an "unknown" person is appropriate. However, because use of the application requires consent except in exigent circumstances, thus limiting its use, the Office concluded that the IUP sufficiently addresses the restrictions related to use of the application.

Retention, Access, and Use of Data; Public Access or Use of Data; and Access to Information and Data by Outside Entities

Since the Digital Fingerprint Scanning Devices IUP states that fingerprint data processed by IDEMIA is not saved, it is unclear whether the IUP's Policies and Procedures Relating to Retention, Access, and Use of Data or Policies and Procedures Relating to Public Access or Use of the Data are applicable to this surveillance technology. If certain policies and procedures in an IUP do not apply to all technologies covered by the IUP, that should be made clear.

The Digital Fingerprint Scanning Devices IUP also does not address whether information regarding a match to NYPD's local AFIS may be contemporaneously shared with an external entity, such as a partner law enforcement agency during the course of an investigation. Of note, the Portable Electronic Devices IUP specifically states that access will not be granted to external entities in furtherance of immigration enforcement.[125]

[122] *Id.*
[123] *Id.*, at 6.
[124] *Id.*, at 5.
[125] *See* N.Y.C. Police Dep't, *Portable Electronic Devices IUP* (Dec. 7, 2023), at 8.

Internal Audit and Oversight Mechanisms

The Digital Fingerprint Scanning Devices and PED IUPs provide a general description of NYPD's internal audit and oversight mechanisms associated with digital fingerprint scanning technology. Both IUPs note, "All NYPD personnel are advised that NYPD computer systems and equipment are intended for the purposes of conducting official business" and, "The misuse of any system or equipment will subject employees to administrative and potentially criminal penalties."[126] The IUP also notes that NYPD conducts internal audits on the local AFIS to ensure fingerprint images connected with sealed criminal cases are expunged from the system.[127] However, there is no indication that the use of IDEMIA is being monitored to analyze use by officer, by frequency of use, by location or command, demographics of individuals on which the technology is being used, or any other quantitative or qualitative metrics. While such monitoring and disclosure of this information would extend beyond the requirements of the POST Act, the Office recommends that NYPD develop mechanisms to closely examine the use of such technology to determine any areas for improvement, and include this information within the IUP.

Disparate Impacts of the Impact and Use Policy

NYPD's Digital Fingerprinting Scanning Devices and PED IUPs technically comply with the POST Act, because the Act requires an IUP to address the disparate impact of the Impact and Use Policy itself, rather than the disparate impact of the surveillance technology on protected groups. As such, the Act does not require NYPD to publicly disclose any disparate impact related to the usage of the IDEMIA application, or any associated digital fingerprinting scanning and portable electronic devices, on protected groups. However, OIG-NYPD takes the position that NYPD should nonetheless include in each IUP the potential disparate impacts of the use and deployment of the surveillance technology itself on protected groups, as NYPD has done for certain, but not all, surveillance technologies.

E. The Augmented Reality ("AR") Application

NYPD's Information Technology Bureau built the AR application, which is capable of visualizing data stored within NYPD databases that are accessible on Department-

[126] *Id.*, at 9. *See also* N.Y.C. Police Dep't, *Digital Fingerprint Scanning Devices IUP* (Apr. 11, 2023), at 11.
[127] *See* N.Y.C. Police Dep't, *Digital Fingerprint Scanning Devices IUP* (Apr. 11, 2023), at 11.

issued phones. This includes the phone's Domain Awareness System ("DAS") application, which links to a centralized repository of information stored in various NYPD databases that contain 911 data, complaint reports, arrest reports, and arrest and warrant histories.[128] The AR application augments the user's smartphone camera to display information contained in DAS.[129] "In the application, the DAS data will be linked to the physical location of where the camera is pointed; the application does not have recording capabilities, nor does it employ facial recognition technology."[130]

In May 2023, NYPD began a pilot program for the AR application in Police Service Area ("PSA") 3.[131] In July 2023, the Department expanded the pilot program to include designated personnel from select commands, including various precincts as well as PSA 3. They were provided access to the AR application on their Department-issued smartphones for a period of three months beginning July 2023 as part of the pilot program.[132] According to NYPD, it planned to conduct an evaluation of the application following the completion of the program. Internal NYPD documents reflect an intention to launch the application citywide in the fourth quarter of 2023, depending on the success of the pilot program.[133] However, NYPD confirmed that the application was not launched citywide until February 16, 2024.

According to NYPD, the PED IUP, as amended by the April 11, 2023 addendum, addresses the AR application. Based on OIG-NYPD's review, it appears that the IUP sufficiently describes the capabilities and use of the AR application. However, OIG-NYPD also concluded that, in certain respects, the IUP does not provide sufficient information about the technology regarding policies and procedures related to data retention and access as required by the POST Act.

Capabilities and Rules, Processes and Guidelines Relating to the Use of the Technology

[128] *See* N.Y.C. Police Dep't, *Domain Awareness System (DAS) IUP* (Apr. 11, 2021), at 3.
[129] *See* N.Y.C. Police Dep't, *supra* note 125, at 4.
[130] *Id.*, at 4.
[131] *See* N.Y.C. Police Dep't, *Operations Order Number 23 – Pilot Program – Augmented Reality Application Within the Confines of Police Service Area 3* (May 2, 2023), at 1.
[132] *See* N.Y.C. Police Dep't, *Operations Order 30 – Expansion of Pilot Program – Augmented Reality Application Within the Confines of the 79th, 81st, 84th, 88th and 90th Precincts and Police Service Area 3* (Jul. 5, 2023).
[133] *See* N.Y.C. Police Dep't, *Project Management Office – NYPD Augmented Reality*, at Proof of Concept.

The April 11, 2023 addendum to the PED IUP stated that the Department launched a pilot program where a "small number" of NYPD-issued smartphones have access to an augmented reality application.[134] According to NYPD, the pilot program allows the application to be deployed at the user's discretion. The IUP does not disclose any policies or procedures related to the use of the AR application and instead provides information in relation to portable electronic devices in general.

Retention, Access, and Use of Data; Public Access or Use of Data; and Access to Information and Data by Outside Entities

Since the AR application has no recording capabilities, the "Policies and Procedures Relating to Retention, Access, and Use of Data" and the "Policies and Procedures Relating to Public Access or Use of the Data" sections of the IUP are not applicable to this new surveillance technology. The IUP should therefore explicitly state that these policies do not apply to the AR application.

The IUP also does not address whether the information contained in DAS, and which is displayed via a smartphone camera using the AR application, may be contemporaneously shared with an external entity, such as a partner law enforcement agency during the course of an investigation, and should be revised to include this information. Of note, the IUP specifically states that access will not be granted to external entities in furtherance of immigration enforcement.[135]

Internal Audit and Oversight Mechanisms

The IUP indicates that the AR application can be employed at the users' discretion.[136] There is no indication that NYPD monitors the application's use by officer, reason for use, frequency of use, or to determine whether the application was, in fact, used as specified in the IUP. While this would extend beyond the requirements of the POST Act, the Office recommends that NYPD develop mechanisms to closely examine the use of such technology to determine any areas for improvement, and include this information within the IUP.

Disparate Impacts of the Impact and Use Policy

NYPD's PED IUP technically complies with the POST Act, because the Act requires the IUP to address the disparate impact of the Impact and Use Policy itself, rather

[134] *See* N.Y.C. Police Dep't, Police Dep't, Portable Electronic Devices IUP (Apr. 11, 2023), at 3.
[135] *See* N.Y.C. Police Dep't, *supra* note 125, at 8. *See also* N.Y.C. Police Dep't, *supra* note 134, at 7.
[136] *See* N.Y.C. Police Dep't, *supra* note 125, at 3.

than the disparate impact of the surveillance technology on protected groups. As such, the Act does not require NYPD to publicly disclose any disparate impact related to the usage of the AR application on protected groups. However, OIG-NYPD takes the position that NYPD should nonetheless include in each IUP the potential disparate impacts of the use and deployment of the surveillance technology itself on protected groups, as NYPD has done for certain, but not all, surveillance technologies.

V. Findings

Based on the Office's review of the new 2023 technologies acquired by NYPD, the applicable IUPs as identified by NYPD, and additional NYPD records and interviews related to the new technologies, OIG-NYPD makes the following findings:

1) NYPD has used grouping in an overly expansive manner by continuing to include Digidog within the existing Situational Awareness Cameras' ("SAC") IUP, rather than issuing an individual IUP, effectively undermining goals of the POST Act and limiting public transparency with respect to Digidog.

2) NYPD's grouping approach creates a risk that individual technologies may be shielded from public scrutiny and oversight, limiting the transparency about these technologies that the POST Act sought to create. To the extent that grouped technologies are unique, this approach deprives members of the public of an opportunity for notice and comment with respect to the applicable IUP, and makes it more difficult for the public to discern the capabilities and use of the technologies and the policies applicable to them.

3) OIG-NYPD continues to maintain, as it did in its 2022 POST Act report, that Digidog is a surveillance technology with distinct capabilities and should have had a separate IUP when it was deployed in 2021. The new Digidogs purchased and deployed in 2023 include enhancements to the prior Digidog, which should have, at a minimum, been addressed in an addendum to the SAC IUP, since there was no separate IUP for Digidog.

4) K5, StarChase, IDEMIA, and the AR application were appropriately identified as enhancements to or new uses of existing surveillance technologies, and therefore, the issuance of an addendum for each technology was sufficient under the POST Act.

5) Nevertheless, while K5, StarChase, IDEMIA, and the AR application were appropriately introduced via addenda in existing IUPs, the IUPs are insufficient because they do not include all of the information required by the POST Act:

a. The SAC IUP does not disclose health and safety information with respect to K5;
b. The GPS Tracking Devices' IUP does not adequately disclose the specialized rules, processes, and guidelines that distinguish StarChase technology from other GPS tracking technologies, health and safety information, or the type of data that may be disclosed to external entities;
c. Neither the Digital Fingerprint Scanning Devices' IUP nor the Personal Electronic Devices' IUP provide sufficient information about IDEMIA with respect to policies and procedures related to data retention and access;
d. The Portable Electronic Devices' IUP does not provide sufficient information about the AR application regarding policies and procedures related to data retention and access.

VI. Recommendations

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

1) NYPD should issue a new individual IUP for Digidog.

2) NYPD should amend the addenda to the IUPs applicable to StarChase, IDEMIA, and the AR application to meet all of the requirements of the POST Act. The GPS Tracking Devices' IUP should be updated to adequately disclose the specialized rules, processes, and guidelines, health and safety impacts, and the type of data that may be shared with external entities in relation to StarChase; the Digital Fingerprint Scanning Devices' IUP should be updated to adequately address policies and procedures related to data retention and access in relation to IDEMIA; and the Portable Electronic Devices' IUP should be updated to adequately disclose policies and procedures regarding data retention and access in relation to the AR application.

3) In the event that NYPD uses K5 in the future, the Department should disclose health and safety information related to the technology within the SAC IUP.

4) For future IUPs, NYPD should group surveillance technologies into single IUPs only when the surveillance technologies at issue are substantially similar in capability and manner of use, and the IUP identifies and specifically names the individual technologies to which specific information within the IUP applies.

5) NYPD should review its existing IUPs, that "group" multiple surveillance technologies to determine if grouping is permissible under the standard set out in Recommendation 4, and issue new IUPs or addenda as appropriate.

6) While not a requirement of the POST Act, NYPD should update the Internal Audit and Oversight sections of its IUPs to include mechanisms for tracking and monitoring use of its surveillance technologies to ensure that the technologies are being used as described in the IUPs, and that the IUPs do not result in a disparate impact on any protected groups.

7) OIG-NYPD continues to maintain, as it did in its 2022 Report, that while not a requirement of the POST Act, NYPD should include in each IUP the potential disparate impacts of the surveillance technology on protected groups (instead of the potential disparate impacts of the IUP on protected groups, as is currently required under the law).

Appendix A: Local Law 65 of 2020

LOCAL LAWS
OF
THE CITY OF NEW YORK
FOR THE YEAR 2020

No. 65

Introduced by Council Members 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:

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

2

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.

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.

3

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;

4

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

THE CITY OF NEW YORK, OFFICE OF THE CITY CLERK, s.s.:

I hereby certify that the foregoing is a true copy of a local law of The City of New York, passed by the Council on June 18, 2020 and approved by the Mayor on July 15, 2020.

MICHAEL M. McSWEENEY, City Clerk, Clerk of the Council.

CERTIFICATION OF CORPORATION COUNSEL

I hereby certify that the form of the enclosed local law (Local Law No. 65 of 2020, Council Int. No. 487-A of 2018) to be filed with the Secretary of State contains the correct text of the local law passed by the New York City Council and approved by the Mayor.

STEPHEN LOUIS, Acting Corporation Counsel.

5