

June 8, 2023

Via Email & U.S. Mail

Acting Inspector General Jeanene Barrett  
Office of the Inspector General for the  
New York City Police Department  
New York City Department of Investigation  
180 Maiden Lane  
New York, NY 10038

Alan Levine  
*President*

Twyla Carter  
*Attorney-in-Chief*  
*Chief Executive Officer*

Justine M. Luongo  
*Chief Attorney*  
*Criminal Practice*

Timothy B. Rountree  
*Attorney-in-Charge*  
*Queens County Office*

Re: NYPD POST Act Compliance Failures

Dear Acting Inspector General Jeanene Barrett,

We write to respectfully request that you open an investigation into the New York City Police Department's adoption of new surveillance technologies in violation of the [Public Oversight of Surveillance Technology \(POST\) Act](#) (Local Law 65 of 2020).

The POST Act requires the NYPD to issue impact and use policies (IUPs) for each surveillance technology it uses.<sup>1</sup> It also requires the NYPD to propose and publish an IUP on the department's website "at least 90 days prior to the use of any new surveillance technology."<sup>2</sup> The public then "shall have 45 days to submit comments on such policy" to the NYPD Commissioner.<sup>3</sup>

On April 11, 2023, the NYPD announced new surveillance technologies it would start using immediately. There were no new impact and use policies issued for these technologies, nor was the mandatory 45 days for the public to comment on them permitted. Seemingly to avoid these requirements, the NYPD updated five of the thirty-six previously issued IUPs to reference the new tools, even though each of these tools are different from the technologies under which the NYPD has categorized them. The updates to the five existing IUPs are inadequate to fulfill the NYPD's responsibility to describe the policies that govern its possession and use of new technologies, in violation of the requirements of the POST Act.

In a press conference with Police Commissioner Keechant Sewell and Chief of Department Jeffrey Maddrey on April 11, 2023, New York City Mayor Eric Adams [announced](#) several new technologies that the NYPD has acquired and intends to use going forward, either in pilot programs or permanently.<sup>4</sup> The Mayor discussed three new technologies:

---

<sup>1</sup> NYC AC § 14-188.

<sup>2</sup> *Id.* at (b).

<sup>3</sup> *Id.* at (e).

<sup>4</sup> "Transcript: Mayor Adams Makes Public Safety Announcement With NYPD Commissioner Sewell," NYC.gov: The Official Website of the City of New York, April 11, 2023. Accessed May 3, 2023. Available at: <https://www.nyc.gov/office-of-the-mayor/news/246-23/transcript-mayor-adams-makes-public-safety-announcement-nypd-commissioner-sewell>

- A K5 autonomous security robot that is intended to patrol a “predetermined path” in areas such as subway stations. According to the Mayor, “the K5 uses self-driving technology. It has onboard cameras and sensors, is similar to like a Roomba, a robot vacuum.”<sup>5</sup>
- A return of Digidog, the dog-like remote-controlled robot that “will be able to enter, assess, assist the NYPD in tracking and investigating high risk hazardous situations and locations.”<sup>6</sup> Chief of Department Madrey stated that the robot “will be deployed to assist ESU, or Emergency Service unit, in hostage negotiations, counter-terrorism incidents, and other situations as needed.”<sup>7</sup> He later stated that Digidog may interact with “people who are suspects in crime” and “people suffering from mental health crisis,” but did not specify how or when these interactions would be allowed.<sup>8</sup> Frank Digiaco, the NYPD’s Technical Assistance Response Unit Commanding Officer, stated that the NYPD paid \$750,000 for Digidog using forfeiture money.<sup>9</sup>
- The StarChase GPS tracking guns.<sup>10</sup> The NYPD is using two different versions of the StarChase GPS gun: a handheld device and a car-mounted device. Each launch a projectile with a live GPS tracker on it at a moving car. The GPS unit can then track the car, ostensibly in lieu of a police chase of the car.

These three technologies, plus two others that were not announced at this press conference, were incorporated into the NYPD’s [existing](#) technology Impact and Use Policies (IUPs) on April 11, 2023. Five existing IUPs were updated, and no new IUPs were added for the new technology acquired by the NYPD.

The two new technologies not announced at the Mayor’s press conference were:

- New digital fingerprint scanning technology that will allow officers to scan fingerprints straight from their cell phones.<sup>11</sup>
- A new “augmented reality” technology available on some NYPD officers’ phones that will allow them to “better visualize that data [contained in the Domain Awareness System].” The

---

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

<sup>10</sup> *Id.*

<sup>11</sup> It is somewhat unclear from the descriptions in the Portable Electronic Device and Digital Fingerprint Scanning Technology IUPs whether this is an entirely new technology or simply an expansion of a technology briefly mentioned in the 2021 version of the IUPs. It is impossible to tell from the vague descriptions of the technology, which is a large part of the problem that this letter highlights.

latter technology was briefly mentioned, though not described in depth, in Commissioner Keechant Sewell's 2023 [State of the NYPD](#) address on January 25, 2023.<sup>12</sup>

In its original assessment of the NYPD's compliance with the POST Act, your office found that the NYPD's IUPs, released in 2021, were deficient in three respects. First, the descriptions were "insufficient to enable OIG-NYPD to conduct full annual audits (as the Act also requires) and to achieve appropriate transparency with the public, consistent with practices in other jurisdictions, as to the nature and use of these technologies."<sup>13</sup>

Second, the NYPD's IUPs used boilerplate language that provided insufficient detail. The POST Act requires that the IUPs address the disparate impact of the technologies, not the disparate impact of the impact and use policies. Of the finalized IUPs, only 15% addressed the disparate impact of the technologies on "any protected groups as defined in the New York City [H]uman [R]ights [L]aw."<sup>14</sup>

Third, the grouping of multiple technologies into single IUPs "limits the information made available to the public concerning the nature and use of individual technologies (to the extent grouped technologies differ)."<sup>15</sup> The NYPD cited "time constraints," "operational considerations," and "the position that the functionality of many of the technologies are the same" for the grouping of technologies into single IUPs as defense for their failure to comply. Your office properly concluded that this is contrary to the intent of the POST Act.<sup>16</sup>

Your report further noted at the time that "NYPD's grouping approach allows it to introduce new technologies under an existing group category covered by an existing IUP, and begin use immediately without the required notification to the public and City Council."<sup>17</sup> That is exactly what happened here.

The report goes on to say:

Furthermore, without more information about the functionalities of the various technologies, OIG-NYPD cannot assess whether NYPD's use of surveillance technologies complies with published IUPs. For instance, the "DigiDog" robot— deployed as part of a pilot program by NYPD— has significant capabilities that potentially overlap with multiple IUP groups. It is

---

<sup>12</sup> Keechant Sewell, "2023 State of the NYPD," YouTube. Uploaded Jan. 25, 2023. Last accessed May 3, 2023. Available at <https://youtu.be/UyZjVz6w1n4?t=2049>.

<sup>13</sup> Office of the Inspector General - NYPD, "An Assessment of NYPD's Response to the POST Act," (hereinafter "OIG-NYPD Report") November 2022, Available at [https://www.nyc.gov/assets/doi/reports/pdf/2022/POSTActReport\\_Final\\_11032022.pdf](https://www.nyc.gov/assets/doi/reports/pdf/2022/POSTActReport_Final_11032022.pdf), last accessed May 11, 2023, at 4.

<sup>14</sup> *Id.* at 5.

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

unclear, from an oversight perspective, which IUP(s) govern the use of this technology, and, if more than one, which aspect of each IUP applies to this robotic device. This lack of clarity underscores the need for an IUP for each specific technology.<sup>18</sup>

The new technologies unveiled in 2023, many of which overlap IUP groups and have information in one IUP group that contradicts information in another, only make clearer how necessary it is for the NYPD to release IUPs for each specific technology. The grouping allows technologies that fall across IUP groups to be described minimally, and for the NYPD to withhold key information about the way these technologies work, the rules for deploying them, and the oversight of their use.

These additions underline a main conclusion of the original OIG-NYPD Report on the POST Act: “the most logical reading of the POST Act’s language is that it requires an IUP for each surveillance technology.”<sup>19</sup>

The inadequacy of the IUPs with respect to each newly announced technology is addressed below.

### **Digidog**

Digidog is one of only two kinds of “situational awareness cameras” that transmit both video and audio, and enable two-way communication between the NYPD and someone standing near the device. Other situational awareness cameras only transmit video, and only one way. This [technology](#) allows not just for passive video collection but also for communication by the NYPD with members of the community when the robot is deployed—a much different type of interactive technology that goes far beyond “situational awareness.”

That data is transmitted by “either an encrypted signal, secure data transmission to/from a cloud, or through a direct wired connection.”<sup>20</sup> The IUP does not specify which of these options applies to Digidog.

Though there are differences between the way that Digidog allows for communication and the way that it transmits data to and from the NYPD, the data retention policy is not specified in the IUP. The SAC IUP states, “[e]xcept for the autonomous security robot, the NYPD does not record, store, or retain any of the video or acoustic data processed by situational awareness cameras.”<sup>21</sup> It is not clear whether or how this policy applies to Digidog, and if not then how data is otherwise recorded, stored or retained.

---

<sup>18</sup> OIG-NYPD Report at 5.

<sup>19</sup> *Id.* at 36.

<sup>20</sup> NYPD, “Situational Awareness Cameras: Impact and Use Policy,” April 11, 2023. accessed May 11, 2023. Available at [https://www.nyc.gov/assets/nypd/downloads/pdf/public\\_information/post-final/situational-awareness-cameras-nypd-impact-and-use-policy\\_4.11.23\\_final.pdf](https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/situational-awareness-cameras-nypd-impact-and-use-policy_4.11.23_final.pdf).

<sup>21</sup> *Id.* at 3.

The rules that govern Digidog appear to be the same as other situational awareness cameras, although that is not specified. Only TARU or ESU can use situational awareness cameras, according to the IUP. To the extent that Digidog is considered a situational awareness camera, the IUP states that the NYPD does not seek court authorization for its use, and it is “only used during exigent circumstances or in emergency environments.”<sup>22</sup> This rule, however, applies to all situational awareness cameras and the specifics of the rules governing the use of Digidog specifically are not laid out in the IUP.

Further, at the press conference announcing the acquisition of Digidog, the NYPD Chief of Department Jeffrey Maddrey stated “[t]his will only be deployed at the direction of the Chief of Department, myself.”<sup>23</sup> That very specific restriction on the use of Digidog is not in any IUP, and contradicts the IUP’s general statement about deployment of SACs, which states that “[u]se of situational awareness cameras is a strategic decision made by ESU or TARU personnel during law-enforcement encounters where ESU or TARU responds to requests for assistance.”<sup>24</sup> The IUP does not lay out any specific safeguards designed to protect information collected by the technology from unauthorized access, and the language is largely boilerplate.

The language referencing which outside entities have access to the data collected by Digidog, as well as language regarding specific training for using Digidog, is largely boilerplate and nonspecific. However, the section on oversight mechanisms references specific ESU and TARU training regarding Digidog: “ESU and TARU personnel are specifically trained in their use and in appropriate application of the cameras.”<sup>25</sup> No further description of the training on Digidog is noted.

The IUP states that there are no reports on the health or safety effects of the technology but does not specify whether any impacts on health or safety of Digidog specifically was considered.

While the IUP states that “[t]he safeguards and audit protocols built into this impact and use policy for NYPD situational awareness cameras mitigate the risk of impartial and biased law enforcement,” it also states that the use of Digidog is a strategic decision by TARU or ESU during law enforcement encounters, without further expanding on how the disparate impact that that may have on protected groups is accounted for in those decisions.<sup>26</sup>

### **Autonomous Security Robot**

---

<sup>22</sup> *Id.* at 4.

<sup>23</sup> “Transcript: Mayor Adams Makes Public Safety Announcement With NYPD Commissioner Sewell” NYC.gov: The Official Website of the City of New York, April 11, 2023. Accessed May 3, 2023. Available at: <https://www.nyc.gov/office-of-the-mayor/news/246-23/transcript-mayor-adams-makes-public-safety-announcement-nypd-commissioner-sewell>

<sup>24</sup> SAC IUP at 8.

<sup>25</sup> SAC IUP at 8.

<sup>26</sup> *Id.* at 8-9.

The autonomous security robot is a more powerful surveillance technology than a situational awareness camera, and is used in different ways.

The autonomous security robot is one of the technologies most in need of its own IUP, as it functions very differently than any other technology the NYPD deploys, and is mentioned specifically in two IUPs – the [Situational Awareness Camera IUP](#) and the [Thermographic Camera IUP](#). The phrase “*except for the autonomous security robot*” is used multiple times across both situational awareness camera and thermographic camera IUPs to distinguish the security robot technology from the other technologies deployed by the NYPD.

For example, the SAC IUP distinguishes between the robot and other situational awareness cameras that do not store audio or video data. “*Except for the autonomous security robot*, the NYPD does not record, store, or retain any of the video or acoustic data processed by situational awareness cameras. The autonomous security robot data will be retained for thirty (30) days.”<sup>27</sup> The IUP does not specify what data from the autonomous security robot will be retained in that 30-day period.

The way in which data is collected and stored by the robot is very different than other cameras, either situational or thermographic, used by the NYPD. Unlike other situational awareness cameras that are manually manipulated, “[c]ameras attached to autonomous security robots [will travel] along pre-programmed routes,”<sup>28</sup> It will then send video and audio data back to the NYPD at a remote monitor either by “an encrypted signal, secure data transmission to/from a cloud, or through a direct wired connection between the situational awareness camera and the monitor.”<sup>29</sup> It is not specified which data transmission method is used for this technology.

The thermographic camera IUP is somewhat more specific, stating, “NYPD thermographic cameras capable of wireless remote viewing transmit thermal images and associated data to a remote monitor over an encrypted signal.”<sup>30</sup> However, whether this applies to the autonomous security robot is not specified.

With regard to rules and policies, the NYPD states “[t]he autonomous security robot data will be retained for thirty (30) days. Situational awareness cameras do not use video analytics, facial recognition, or any other biometric measuring technologies.”<sup>31</sup> That statement is false as applied to the autonomous security robot, which *does* use thermographic technology. The TC IUP

---

<sup>27</sup> *Id.* at 3.

<sup>28</sup> *Id.*

<sup>29</sup> SAC IUP at 3.

<sup>30</sup> NYPD, “Thermographic Cameras: Impact and Use Policy,” (hereinafter “TC IUP”) April 11, 2023. Accessed May 11, 2023. Available at: [https://www.nyc.gov/assets/nypd/downloads/pdf/public\\_information/post-final/thermographic-cameras-nypd-impact-and-use-policy\\_4.11.23\\_final.pdf](https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/thermographic-cameras-nypd-impact-and-use-policy_4.11.23_final.pdf) at 5.

<sup>31</sup> SAC IUP at 5.

acknowledges that thermographic cameras process “infrared light emitted by a person or object,” which is a biometric measuring technology.<sup>32</sup>

The thermographic camera IUP also suggests that the autonomous security robot retains this biometric information. “[e]xcept for the autonomous security robot, the NYPD does not record, store, or retain any of the heat signature video images or temperature data processed through the use of thermographic cameras. The autonomous security robot data will be retained for thirty (30) days.”<sup>33</sup>

The training section of both the SAC IUP and the TC IUP contradict themselves with regard to the autonomous security robot, because the use of the technology is so different from the other technologies covered by either IUP. The situational awareness camera training section states that only ESU or TARU are authorized to use the situational awareness cameras, and “[u]se of situational awareness cameras is a strategic decision made by ESU or TARU personnel during law-enforcement encounters where ESU or TARU responds to requests for assistance.”<sup>34</sup> This does not seem to apply to the autonomous security robot, which constantly patrols and “will be used to provide additional public safety resources and help deter crime.”<sup>35</sup> Despite this conflicting use, there are no details on which members of the NYPD will be trained to use this technology or how they will be trained.

Both IUPs that reference the security robot claim there are no health or safety concerns with any technology but do not take specifically into account that an “autonomous” “robot” will be let loose in a busy commuter and tourist thoroughfare and will move independently of any NYPD personnel.

The disparate impact section of the situational awareness camera IUP repeats the claim that “NYPD situational awareness cameras do not use video analytics or any biometric measurement technologies,” with no mention of the fact that the autonomous security robot does use biometric measurement technology. Similarly, the thermographic camera IUP states that “The NYPD does not record, store or retain any heat signature video or temperature data created by thermographic cameras.”<sup>36</sup> However, it is repeatedly stated elsewhere in the IUP that the autonomous security robot stores thermographic data for 30 days. No disparate impacts of the autonomous security robot specifically are addressed in either IUP.

In contrast to the treatment of the autonomous security robot, the thermographic cameras IUP briefly mentions “the thermographic cameras equipped to manned and unmanned aircraft systems,” but states because they are “integrated into a more intricate system,” those technologies are covered in

---

<sup>32</sup> TC IUP at 3.

<sup>33</sup> *Id.* at 5.

<sup>34</sup> SAC IUP at 8.

<sup>35</sup> *Id.*

<sup>36</sup> TC IUP at 5.

separate IUPs.<sup>37</sup> The autonomous security robot is clearly an intricate system with its own uses, rules, and policies and should be treated as such.

### **GPS Gun**

In the NYPD's [Global Positioning Satellite Technology IUP](#) ("GPS IUP"), there is no specific description of the capabilities of the new pilot "Star Chase" technology.<sup>38</sup>

The IUP states that all GPS technology, except for the Star Chase technology, is part of a closed network. However, "[f]or GPS tracking devices used on fleeing vehicles, data is stored in a secure cloud environment."<sup>39</sup> Because of the different way that the data is stored, the data retention policies of the Star Chase GPS data, and how that differs from other GPS data obtained by the NYPD, is difficult to discern. The IUP states:

After location data is downloaded and provided to the assigned NYPD investigator, the location data is deleted from the GPS tracking device and connected hardware and software. For GPS tracking devices used to track fleeing vehicles, 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.<sup>40</sup>

This paragraph leaves open two questions: who can access the software while Star Chase is in use, and which location data will be retained for three years? It is unclear from this paragraph whether all GPS data is retained for three years or only Star Chase data.

The remainder of the GPS IUP is non-specific as to the Star Chase technology. It does not say how officers will be trained on the new technology, who will be able to use the new technology, or have any specifics about the oversight mechanisms for use of this technology, despite this technology being put forth as for use in exigent circumstances, in direct contrast to other GPS technologies, which require judicial review.

### **Digital Fingerprint Scanning**

The NYPD has introduced new digital fingerprint scanning technology to some department-issued smartphones. This technology can be accessed by certain NYPD personnel assigned to the Criminal

---

<sup>37</sup> *Id.*

<sup>38</sup> NYPD, "Global Positioning System Tracking Devices: Impact and Use Policy," (hereinafter "GPS IUP") April 11, 2023. Accessed May 11, 2023. Available at: [https://www.nyc.gov/assets/nypd/downloads/pdf/public\\_information/post-final/global-positioning-system-gps-tracking-devices-nypd-impact-and-use-policy\\_4.11.23\\_final.pdf](https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/global-positioning-system-gps-tracking-devices-nypd-impact-and-use-policy_4.11.23_final.pdf).

<sup>39</sup> GPS IUP at 5.

<sup>40</sup> GPS IUP at 6.



Justice, Detective, Patrol, Transit, and Housing Bureaus, which “allows for identification confirmation.”<sup>41</sup>

The [Digital Fingerprint Scanner IUP](#) (“DFS IUP”) additionally states that, “The mobile fingerprint scanning application performs the same function as the physical equipment, but the fingerprint is transmitted only for comparison within the NYPD local AFIS and not to the state or national AFIS. Fingerprints obtained using the mobile fingerprint application are not saved in either the application or locally, on the device itself.”<sup>42</sup>

The intended use includes “the identification of deceased and/or unknown persons, and to confirm the identity of a person for issuance of a summons in the field.”<sup>43</sup> The statement that patrol, transit, and housing police may use the devices to identify “unknown persons” for unspecified reasons is a vague catchall that suggests that the NYPD may use this technology on almost anyone for any reason, with or without legal justification for doing so.

There are no details as to training or oversight of the specific mobile digital fingerprint technology in either the [Portable Electronic Devices](#) or Digital Fingerprint Scanner IUPs.

Additionally, the disparate impact statement in the Personal Electronic Device IUP falsely states that “NYPD PEDs do not use facial recognition or any other biometric measurement technology beyond the fingerprint/facial recognition feature that can be used by NYPD personnel to unlock some PEDs,” ignoring that some PEDs now do allow for biometric measurement of civilians in the field.<sup>44</sup>

### **Augmented Reality App**

There is almost nothing in the updated IUPs referring to the new “augmented reality” technology that some officers will be able to access on their department-issued smartphones.

The [Portable Electronic Device IUP](#) states that, “[a] small number of NYPD-issued smartphones have access to an augmented reality application as part of a pilot program, in which the smartphone camera display will be augmented to better visualize the data contained in DAS. 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.”<sup>45</sup> A footnote

---

<sup>41</sup> NYPD, “Portable Electronic Devices IUP: Impact and Use Policy,” (hereinafter “PED IUP”) April 11, 2023. Accessed May 11, 2023. Available at: [https://www.nyc.gov/assets/nypd/downloads/pdf/public\\_information/post-final/portable-electronic-devices-ped-nypd-impact-and-use-policy\\_4.11.23\\_final.pdf](https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/portable-electronic-devices-ped-nypd-impact-and-use-policy_4.11.23_final.pdf) at 4.

<sup>42</sup> NYPD, “Digital Fingerprint Scanner IUP: Impact and Use Policy,” (hereinafter “DFS IUP”) April 11, 2023. Accessed May 11, 2023. Available at: [https://www.nyc.gov/assets/nypd/downloads/pdf/public\\_information/post-final/digital-fingerprint-scanning-devices-nypd-impact-and-use-policy\\_4.11.23\\_final.pdf](https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/digital-fingerprint-scanning-devices-nypd-impact-and-use-policy_4.11.23_final.pdf) at 4-5.

<sup>43</sup> *Id.* at 5.

<sup>44</sup> PED IUP at 9.

<sup>45</sup> *Id.* at 3.

links to a YouTube video containing a small portion that touches on this technology but gives no details as to how it works or who has access.

There is nothing specific on this technology's data retention policies, who has access (internally or externally), who is trained or by whom, or any audit or oversight mechanisms for this technology in any IUP.

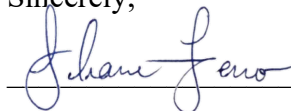
This oversight is a clear violation of the POST Act.

### **Conclusion**

The NYPD introduced five new technologies in 2023 in violation of the POST Act. These technologies were not introduced 90 days before they went into use, and no 45-day public comment period was offered. Though many of the technologies are new and differ in impact and use to other surveillance tools already in use by the NYPD, no new Impact and Use Policies were released by the department. Instead, the NYPD inserted scattered references to the new technologies into existing IUPs. The updated IUPs leave open many questions about the rules governing these new technologies' use, the oversight of these technologies, and the impact they will have on the community. This is a clear violation of both the statutory language and the intent of the POST Act.

The Legal Aid Society would be happy to discuss these issues further with your office and answer any questions you may have.

Sincerely,

A handwritten signature in cursive script that reads "Shane Ferro". The signature is written in black ink and is positioned above a horizontal line.

Shane Ferro  
The Legal Aid Society  
Phone: 347-978-6066  
Email: sferro@legal-aid.org

Cc: NYC Council Speaker Adrienne E. Adams (Via Email & U.S. Mail)  
NYC Council Public Safety Committee Chair Kamillah Hanks (Via Email & U.S. Mail)  
Assistant Deputy Director of the New York City Council's Compliance Unit — Legislative  
Division Malcom M. Butehorn (Via Email & U.S. Mail)