THE
LEGAL AID
SOCIETY
CRIMINAL
DEFENSE

199 Water Street
New York, NY 10038
(212) 577-3300
https://www.legalaidnyc.org/

John K. Carroll
President

Janet E. Sabel
Attorney-in-Chief
Chief Executive Officer

Justine M. Luongo
Attorney-in-Charge
Criminal Practice

February 25, 2021

Submitted via postact@nypd.org

Via Email & U.S. Mail
NYPD Commissioner Dermot Shea
New York City Police Department
One Police Plaza
New York, NY 10038-1497

Via Email & U.S. Mail
DOI Commissioner Margaret Garnett
City of New York
Department of Investigation
180 Maiden Lane
New York, NY 10038-4925

Re: Comments on the NYPD Jan. 11, 2021 Draft Impact & Use Policies, pursuant
to the Public Oversight of Surveillance Technology (POST) Act

Dear Commissioners Shea & Garnett:

The thirty-six draft surveillance technology impact and use policies posted on January 11, 2021, in alleged compliance with the Public Oversight of Surveillance Technology (POST) Act, are so vague and incomplete that they fail to fulfill the POST Act's requirements and contribute little to that legislation's stated purpose of created transparency and greater public understanding around invasive electronic surveillance technologies that have been used disproportionately against Black and brown New Yorkers.

On June 18, 2020, the Council of the City of New York overwhelmingly passed the POST Act,[1] 44-6. Less than a month later, Mayor Bill de Blasio signed it into law,[2] starting the 180-day clock for the NYPD to publicly post for comment draft policies for its existing electronic

[1] Int. No. 0487-2020 (Version A), available at https://legistar.council.nyc.gov/View.ashx?M=F&ID=8730047&GUID=82AE59A1-71F6-42C9-B3E4-5976FF2CA764 [last accessed Feb. 13, 2021].

[2] Local Law No. 65 of 2020, available at https://legistar.council.nyc.gov/View.ashx?M=F&ID=8730045&GUID=222A9417-A45C-4421-B97C-7AD02BEA380A [last accessed Feb. 13, 2021]. Codified into statute under NYC Administrative Code § 14-188 and NYC Charter § 803(c-1).

surveillance technologies covered by the Act. The NYPD posted thirty-six draft policies on January 11, 2021.[3]

The goal of the POST Act was the bare minimum oversight of the invasive surveillance tools that the NYPD has used with little to no input from the public. Transparency around policing practices should not be controversial. Yet it appears from the facial insufficiency of the draft policies that the NYPD has followed its active opposition to the passage of the POST Act with passive resistance to compliance with the spirit and the letter of the law.

Instead of commenting on each draft policy separately, this letter is a response to all the policies posted on January 11, 2021. It also identifies policies that should have been included but were not. The comments are divided into three sections: General Comments, Specific Comments, and Missing Policies. The General Comments cover themes common to many or all of the policies, such as the use of voluminous boilerplate text that provides little insight into any technology and serves only to bolster the length of the policies and lend the illusion of substance. The Specific Comments address issues unique to a particular technology.[4] The Missing Policies section identifies technologies that we are aware the NYPD possesses and/or uses but that were not covered by the policies released thus far.

I. General Comments

A. Necessary Terms Are Not Defined

Throughout the draft policies posted on January 11, 2021, the NYPD refers to “artificial intelligence, machine learning, facial recognition, and any other biometric measuring technologies” but fails to define these terms, making accurate interpretation of the draft policies impossible. For example, while the NYPD denies that some of these potentially problematic technologies are used, it is impossible to determine the accuracy of those denials without a clear, shared understanding of

[3] New York City Police Department, *Draft Policies for Public Comment*, NYC.gov, available at https://www1.nyc.gov/site/nypd/about/about-nypd/public-comment.page [last accessed Feb. 13, 2021].

[4] This letter does not specifically address the Criminal Group Database and Social Network Analysis Tools draft policies. Legal Aid’s comments on those specific policies are addressed in a separate joint letter with the Bronx Defenders, Center for Constitutional Rights, and NAACP Legal Defense and Educational Fund, Inc. Nonetheless, the General Comments provided in this letter apply equally to those policies.

what the NYPD intends by such terms. While these terms may be understood to mean something specific to the NYPD, there are conflicting definitions available for each. Defining these terms, as part of the policies, would provide a better understanding of the capabilities of the NYPD's electronic surveillance technologies and the potential problems that may exist with each.

B. Lack of Vendor Information

Consistent with the NYPD's history of opaqueness surrounding its surveillance contracts and funding, the January 11, 2021 draft policies are missing information as to the vendors, models, versions, etc. of the technologies that the policies purport to cover. It is our understanding that most of the NYPD's surveillance technology is purchased through the Special Expense Budget (SPEX). In 2007, the NYPD entered into an agreement with the Law Department, the Mayor's Office of Contract Services, the Department of Investigation, the City Comptroller's Office, and the Office of Management and Budget, to hide NYPD SPEX budget contracts from the people of the City of New York, despite the general legal requirement for public agency contracts to be public.[5]

The City Comptroller's Office terminated its participation in this agreement on August 27, 2020.[6] Regarding NYPD surveillance purchases, the Comptroller determined that "[t]he POST Act will help to bring some light to those technologies, and in doing so it will also render moot a significant amount of the secrecy that the department has long insisted on bringing to the procurements it designates as classified, confidential special expenses."[7] Despite the Comptroller's assessment and the lack of legitimate justification to continue to hide which companies the NYPD contracts with, the draft policies are bereft of vendor names, model types, software and hardware versions, and other identifying details that are necessary for transparency. This information should be added to the policies.

[5] March 27, 2007 Special Expense Protocol Memorandum of Understanding and June 18, 2010 Amendment to Special Expense Protocol, obtained by the Legal Aid Society via a Freedom of Information Law request, available at https://docdro.id/3kfgo0q [last accessed Feb. 22, 2021].

[6] Rocco Parascandola, *Comptroller Stringer tells NYPD surveillance technology expenses can't be kept secret*, NY Daily News, July 31, 2020, available at https://www.nydailynews.com/new-york/ny-nypd-budget-classified-stringer-20200731-55pwpwz4qzac7hyptmzlre5qyu-story.html [last accessed Feb. 8, 2021].

[7] July 30, 2020 Letter from NYC Comptroller Scott M. Stringer to NYPD Commissioner Dermot Shea, obtained by the Legal Aid Society via a Freedom of Information Law request, available at https://docdro.id/aSYzGho [last accessed Feb. 22, 2021].

C. Safeguard & Security Measures Against Unauthorized Access

The draft policies detail the efforts the NYPD makes to ensure that information or data obtained through its use of surveillance technology remain internally protected from unauthorized use by NYPD employees. However, the draft policies are silent on the efforts the NYPD makes to ensure such information or data remain secure from external (i.e., non-NYPD affiliated) malefactors or, alternatively, misuse by otherwise authorized third parties. Since the information or data generated by the NYPD's use of surveillance technology is both sweeping in its breadth and intimate in its ability to monitor everyday aspects of a New Yorker's life, the omission of such information is concerning.

In this respect, the draft policies fail to comply with the POST Act's provision that the NYPD detail "safeguards or security measure designed to protect information…from unauthorized access" in its surveillance policies. The use of the term "unauthorized access" in the Act is clearly meant to apply to both internal security measures and any cybersecurity measures the NYPD takes to protect information or data generated through its use of surveillance technology from access by actors outside of the NYPD. Otherwise, the Act would have specified that the NYPD promulgate only those policies that relate to internal security.

This omission is especially concerning since data generated using the NYPD's surveillance technology has come under direct attack by non-NYPD affiliated actors. As recently as late 2019, the NYPD was forced to take its entire fingerprint database offline due to the threat of a ransomware attack. Malware was introduced into the NYPD's network by a contractor who was installing a digital display. Once the malware was introduced into the NYPD's system, it spread rapidly to 23 other NYPD computers connected to the NYPD's fingerprint tracking system, forcing the NYPD to reinstall software on 200 computers throughout the city.[8] Ransomware attacks are especially dangerous; had the attack proved successful, precise biometric data on NYC residents could have become the subject of an extortion attempt. Additionally, former Police Commissioner Raymond

[8] *See* Tara Seals, *NYPD Fingerprint Database Taken Offline to Thwart Ransomware*, ThreatPost, Nov. 25, 2019, available at https://threatpost.com/nypd-fingerprint-database-ransomware/150592/ [last accessed Feb. 17, 2021].

Kelly stated in 2009 that the NYPD's computer system faced at least 70,000 hacking attempts per day by international hackers.[9]

Given the increased sophistication of international hackers since 2009 (as evidenced by the successful 2016 hacking of the Democratic National Committee and the successful 2020 SolarWinds cyberattack on U.S. governmental institutions), the NYPD's failure to describe – even generically – how it hardens its network against the possibility of breaches by external actors is deeply troubling. Importantly, it also demonstrates how the uniform language of the draft policies fails to address the POST Act's justifiable insistence that the NYPD's surveillance policies include some information as to how the NYPD protects the data generated through its surveillance from external attacks.

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

The draft policies either lack detailed information on time limitations for retained data or outline retention periods far beyond what is legally appropriate, including, in some cases, indefinite retention. These policies fail to justify both the length of time data is retained and why certain data is retained indefinitely. They do not address how the NYPD balances civil liberty and privacy concerns of individuals whose data is collected, even where the NYPD concedes that the data is subject to deletion pursuant to statute or other court order. The policies also fail to provide time limitations on the ability of authorized personnel to access the data, where that information is accessible through a variety of databases. No justification is provided for the difference in policy.

Much of the information collected is stored in multiple databases. Many of the draft policies make clear that data may be purged from one database but provide no information about whether the data is entirely purged and no longer available through any avenue, including other databases where the information may be cross-referenced. For example, the NYPD concedes that iris scans must be deleted pursuant to statute but freely admit that they remain accessible in another database, seemingly forever, and accessibly by other NYPD personnel. This implicates not only internally authorized users that may differ across databases, but external entities granted access to different

[9] *See* Associated Press, *Hackers Attack NYPD Computers 70K Times Per Day*, NBC New York, Apr. 23, 2009, available at https://www.nbcnewyork.com/news/local/nypd-computers-targeted-by-international-hackers/1893248/ [last accessed Feb. 17, 2021].

databases, and the difference in policy regarding release of information from one database, versus another, to the public. While some policies contain provisions regarding limited authorization to access certain databases, there are no specific policies outlining how access is revoked. This is especially problematic considering the vague FOIL policies associated with each of the draft policies. To conform with the requirements of the POST act, the policies should, at minimum, provide details on specific time limitations for retention, clear rules of access, and the safeguards put in place to ensure that the data is purged from all databases. They must also provide justification for each of these aspects of the policies.

E. External Entities

The boilerplate language used in each of the draft policies on the NYPD's information sharing with external entities is plainly insufficient to meet the mandates of the POST Act. The Act explicitly provides that the NYPD's surveillance policies detail each entity with whom the NYPD shares information, including whether each entity is a "local governmental entity, a state governmental entity, a federal governmental entity, or a private entity." The Act further requires that the NYPD's surveillance policies detail the "type of information and data that may be disclosed by *such* entity" and "any safeguards or restrictions imposed by the department on *such* entity regarding the use or dissemination of the information collected by such surveillance technology" (emphases added). The draft policies fail to meet these requirements, referring only generically to other governmental entities and vendors with whom the NYPD shares information and/or data. No specific external entity is ever named in the draft policies.

The draft policies further fail to detail, with any specificity whatsoever, the type of information and/or data that the NYPD shares with external entities. Given the NYPD's failure to specify the entities with which it shares data, this omission is unsurprising; however, this still means that the NYPD has failed to comply with the Act's provisions. Further, the draft policies fail to specify the particular "safeguards or restrictions" they impose on each entity with whom the NYPD shares information and/or data. Instead, the draft policies refer generically to granting access to external entities on a "case by case basis," subject to the terms of unspecified agreements with said external entities. This practice is a far cry from the Act's mandate that the NYPD affirmatively detail the precise safeguards and restrictions it imposes on each external entity with whom it shares data, within the context of each policy (i.e., regarding the surveillance technology that the policy addresses). The Act requires more than simply referring to the concept of having access and confidentiality agreements with unspecified external entities; instead, such access and confidentiality agreements should be addressed with a modicum of particularized detail.

As the draft policies stand, no member of the public would be adequately and appropriately apprised of which entities the NYPD shares information or data with, the type of information or data shared with each entity, and the controls that the NYPD imposes upon each entity regarding further disclosure of any shared information or data. The NYPD, at the very least, shares information or data with federal governmental agencies given its participation in the federal Fusion Center program, through the New York State Intelligence Center, as well as its participation in the federal Joint Terrorism Task Force program.[10] The NYPD also shares information or data with foreign governmental entities through its International Liaison program.[11]

Thus, at the very least, each draft policy must be revised to detail which federal or foreign entities the NYPD shares information with, what information or data derived from the relevant surveillance technology is shared with those specific federal or foreign entities, and the access and confidentiality safeguards it has put into place regarding the data derived from the relevant surveillance technology that it shares with these federal and foreign entities. This is merely a starting point to bring the NYPD in compliance with the Act, as the NYPD assuredly shares information or data derived from its use of surveillance technology with other local and state governmental entities (e.g., through the State's Counterterrorism Law Enforcement Liaison Unit) and with non-governmental entities (through the NYPD SHIELD program).[12] Policies compliant with the Act

[10] *See* Michael Price, *National Security and Local Police*, Brennan Center for Justice, 2013, available at https://www.brennancenter.org/sites/default/files/2019-08/Report_NationalSecurity_LocalPolice.pdf [last accessed Feb. 17, 2021].

[11] *See* The New York City Police Foundation, *Counterterrorism*, available at https://www.nycpolicefoundation.org/programs/counterterrorism/ [last accessed Feb. 17, 2021].

[12] *See* New York State Division of Homeland Security and Emergency Services, http://www.dhses.ny.gov/oct/units/law-enforcement/ [last accessed Feb. 17, 2021]; NYPD SHIELD Operation Nexus, http://www.nypdshield.org/public/nexus.aspx [last accessed Feb. 17, 2021].

would sufficiently detail how data derived from each surveillance technology the NYPD uses is shared with each entity with whom it has entered into information-sharing agreements. In their current state, the draft policies provide no substantive insight into how the NYPD shares information with external entities.

F. Training

The POST Act requires NYPD to state whether any training is required to for an individual to use a specific surveillance technology or access the information generated from such a technology. The draft Impact and Use Policies disseminated by NYPD are insufficient to inform the public what training is required to use these surveillance technologies and whether NYPD is providing appropriate training oversight. The draft policies frequently repeat that "command level" training is provided on a specific technology. However, the policies do not include any details as to the provided training. They do not discuss whether the training solely focuses on the operation of the technology or also includes instruction on the significant legal and privacy issues surrounding most of these technologies. They do not differentiate between technologies that require an initial training or those that require periodic updating. The draft policies also include rote statements that the applicable surveillance technology must be operated in compliance with NYPD policies and training. However, because the policies fail to explain or describe either the policies or the training, this statement is meaningless. Without the public having insight into the relevant training, it is impossible to know if NYPD is complying with their training or whether that training provides any grounds for confidence in the reasonableness of the NYPD's use of such technology.

Additionally, it is unclear if these training programs incorporate protections to prevent biased or racially disparate policing. Surveillance technology has often been leveraged against people of color and historically discriminated groups.[13] It is important that NYPD account for not only the disparate impact of these technologies, but also how they intend to address this impact through training and other oversight policies. These should be included in the draft policies.

[13] *See* Sidney Fussell, *How Surveillance Has Always Reinforced Racism*, Wired, June 19, 2020, available at https://www.wired.com/story/how-surveillance-reinforced-racism/ [last accessed on Feb. 12, 2021].

The POST Act was passed to provide "comprehensive reporting and oversight" of NYPD. By failing to provide detailed descriptions of the type and extent of training, the draft policies fail to abide with the spirit and letter of the law.

G. Internal Audit & Oversight Mechanisms

The sections of the draft policies addressing internal audit and oversight mechanisms do not provide enough information for any member of the public to assess whether the measures in place are sufficient. Even when the policies require an audit, they are devoid of any information demonstrating that the audit will be conducted with any regularity by competent personnel. Additionally, the policies often fail to list whether logs are kept, by whom, the information contained within them, and the ease in which appropriate supervisors can access them to conduct reviews. Moreover, the policies refer to unspecified checks of computer systems and equipment, without any particularity on how such checks are conducted or how they are designed to reveal misuse and abuse.

Generic claims of appropriate internal checks and balances, which amount to "trust us," are not enough to deliver the transparency the POST Act was meant to provide. It is necessary to have robust descriptions of documentation, either auto-generated or manually created, that will be reviewed at regular intervals, along with surprise inspections, by well trained staff, who will also be held accountable for their failures.

H. Disparate Impacts of the Impact & Use Policies

Each of the draft policies proposed by the NYPD rely upon the assertion that, "[t]he NYPD is committed to the impartial enforcement of the law and to the protection of constitutional rights." They further go on to detail that "[r]ace, color, ethnicity, or national origin may not be used as a motivating factor for initiating police enforcement action." This boilerplate language is plainly insufficient to meet the mandates of the POST Act to address "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," and yet many of the policies make no mention of disparate impact other than that boilerplate language.

As a result, the draft policies in general fail to address the inherent bias built into many of these technologies or engage with any of the well-established criticisms, particularly of technologies built on machine learning and algorithmic decisionmaking, which are known to be built on data sets that reflect past patterns of bias and implicit and explicit bias of the human beings who created them. They also rely on generalized legal prohibitions on explicit bias, which does little to address potential disparate impacts of policing practices on protected groups.

To address these concerns, at a minimum the policies must provide greater detail about each specific technology and what, if any, information is available about the disparate impact of those technologies, including specifics about vendors and steps those entities have taken to identify and address disparate impacts in their products. The policies should also create a system for the NYPD to track disparate impacts in use of these digital technologies – including the race, ethnicity, age, and gender of all individuals subject to the technologies, as well as location information where appropriate – so that there is a proactive approach to identifying and addressing disparate impact. Such information should be made public at regular intervals to enable democratic oversight of these controversial policing practices.

II. Specific Comments

A. Body-Worn Cameras

While the NYPD frequently highlights the body-worn camera program as a tool primarily for "improving and enhancing the safety of officer and civilian interactions" and evidence collection, the NYPD's current BWC program emerged as a court-mandated accountability and transparency measure. Body-worn cameras, when deployed and regulated properly, may contribute to accountability and transparency, but the Body Worn Camera Impact and Use Policy (BWC IUP) fails to achieve that goal.

As the largest provider of legal services in New York City, Legal Aid's attorneys review a significant amount of BWC footage on a regular basis throughout the five boroughs. Our collective experience of the BWC program points to considerable operational issues that detract from the overall usefulness of BWC footage both as evidence and as an accountability mechanism. Attorneys across our various practices regularly report that BWC videos are incomplete records of police interactions with the public. Crucial events, such as witness statements or warrant searches, that do not appear to fall under any exemption are not always captured on BWC footage. Officers turn on cameras too late or not at all. They use their bodies to obstruct one another's cameras, sometimes in a manner that appears intentional. These observations mirror findings reported by the CCRB in a recent report on the NYPD's BWC program.[14] CCRB reported that officers often failed to properly use their cameras by turning it on law, turning it off early, or not turning on the BWC at all, in violation of the NYPD's Patrol Guide.

The BWC IUP fails to address these issues. It fails to include relevant details such as who and how one determines that a BWC was not used according to policy or an overall strategy to address improper use of BWCs. It also fails to address deficiencies in policy that contribute to this problem, including the fact that P.G. 212-123 does not explicitly instruct officers to ensure that BWCs remain unobstructed while recording; that current BWC policy allows officers a wide breath of discretion that obfuscates the cause of inconsistencies in activation; and that officers are able to avoid discipline for non-compliance by claiming vague exemptions to the rules requiring recording. The policy also fails to provide the public with sufficient information about training that could help inform an assessment of whether inadequate training contributes to these issues. For example, it is unclear if the situational training referenced in the IUP adequately reflect the complexities of real-life scenarios or reinforces the training on investigative encounters necessary for their proper use.

There is scant mention of how the maintenance of BWC devices is audited to ensure the integrity of the devices and to guard against malfunctioning during its use. There is no information on steps required to be taken to ensure maintenance of devices by Integrity Control Officers. There also appear to be no procedure to ensure that every member of service that is required to wear BWC, is actually equipped with a properly operating device for their shift. It is also unclear what is done to guard against malfunctions, and what policies are in place to rectify situations when malfunctions do

[14] Civilian Complaint Review Board, *Strengthening Accountability: The Impact of NYPD's Body-Worn Camera Program on CCRB Investigations*, Feb. 2020, available at https://www1.nyc.gov/assets/ccrb/downloads/pdf/policy_pdf/issue_based/20200227_BWCReport.pdf [last accessed Feb. 23, 2021].

occur. There is no mention of logistical difficulties that may arise like low battery life of the device or sudden failure of the device during an officer's shift or overtime. Finally, there is very little information about the extent of involvement that outside vendors have with NYPD in the maintenance and servicing of the devices.

The policy also suffers from specific failures, including the failure to list which specialized units use or do not use body-worn cameras while performing their duties and to justify the exclusion of certain units and ranks, such as the Warrant Section[15] and certain detectives, from the body-worn camera program. Such information is important for the public to establish appropriate expectations regarding what sort of encounters are subject to recording and when BWC footage should and should not be available.

The policy also contains some apparent errors or misstatements of fact. The "Capabilities of the Technology" section of the BWC IUP, for example, states that BWCs "do not use artificial intelligence, machine learning, video analytics, or any kind of biometric measurement technologies."[16] But the NYPD has publicly indicated that BWC footage is used in conjunction with facial recognition, which is a biometric measurement technology. The NYPD's IUP on facial recognition states:

> Images obtained from body-worn cameras worn by NYPD officers are not routinely submitted for facial recognition analysis. For example, the NYPD does not use facial recognition technology to examine body-worn camera video to identify people who may have open warrants. However, if an officer, whose body-worn camera is activated, witnesses a crime but is unable to apprehend the suspect, a still image of the suspect may be extracted from body-worn camera video and submitted for facial recognition analysis.[17]

We urge NYPD to clarify this point and provide a full accounting of what footage and still images from footage produced by BWCs may be used for. This would include, but is not limited to,

[15] We highlight the exclusion of the Warrant Section given the clear potential for unpredictable events and/or unconstitutional policing. In the wake of many high-profile deaths connected to warrant servicing, such as Breonna Taylor and Kathryn Johnston, members of the public have a justifiable expectation that officers would be equipped with a body-worn camera in such scenarios.

[16] BWC IUP p. 1

[17] FIS IUP p. 3

whether BWC footage is used in connection with the operation of the criminal group database, Domain Awareness System, social network analysis tools, and other NYPD technologies.

Finally, the section of the BWC IUP policy concerning access and use of BWC data leaves unanswered many questions regarding who may access footage. The statement that "Authorized users consist only of NYPD personnel in various commands." and only to "execute their lawful duties"[18] is vague given the sheer size and organizational complexity of the NYPD and does not appear to place any meaningful limit on the ability to access and use footage. Given the many privacy concerns surrounding BWC footage, this section would also benefit from an explanation of instances where BWC footage may be made accessible to specialized units and commands within the Department, such as the Intelligence Bureau.

In short, this BWC IUP fails to provide the requisite transparency contemplated by the POST Act for the largest BWC program in the United States. These failures suggest the NYPD has not appropriately investigated the scope, scale, and impact of its BWC program.

B. Communication Assistance for Law Enforcement Act (CALEA) Collection System

Throughout the CALEA Collection System draft policy the NYPD conflates pen register and trap-and-trace (PRTT) orders and eavesdropping warrants. While some of this may be chalked up to an inartfully worded policy, it is consistent with the NYPD's approach in seeking these remedies from the courts. Members of the NYPD, in conjunction with prosecution offices, often apply for the collection of telephone numbers and IP addresses, at the same time as the covert capture of telecommunications content (e.g. voice calls and text messages) and location data. The standards and legal requirements for PRTT orders, search warrants, and eavesdropping warrants are not the same, nor should they be used interchangeably.

In regards to an eavesdropping warrant, the NYPD acknowledges that an investigator "first obtains court authorization allowing for the use of the CALEA collection system to aid an ongoing investigation…The warrant must contain a finding of probable cause by a judge, as well as an

[18] BWC IUP p. 4

explicit authorization for use of the CALEA collection system for a specified period of time." However, the policy fails to mention that New York Criminal Procedure Law Article 700 requires more than just a finding of probable cause and a time limitation. There are numerous restrictions on eavesdropping warrants that are not required for either standard search warrants[19] or for PRTT orders.[20] One of the more important restrictions is that an eavesdropping warrant cannot be issued unless there is "a showing that normal investigative procedures have been tried and have failed, or reasonably appear to be unlikely to succeed if tried, or to be too dangerous to employ."[21] The policy should require, at minimum, guidance for the steps or investigative techniques that must be attempted before a member of the NYPD applies for an eavesdropping warrant. In situations in which a "normal investigative procedure" cannot be tried because it is "unlikely to succeed" or would "be too dangerous to employ", the relevant investigator should be required to document, in written detail, the reasons that such procedures cannot be tried.

Furthermore, the policy allows for the CALEA collection system to be used "without first obtaining a warrant if exigent circumstances exist." It then describes the circumstances, which must exist to justify the warrantless use of the collection system. There are multiple issues with this part of the policy. First, the eavesdropping warrant statute already has a specific procedure to follow when there is an "emergency situation where imminent danger of death or serious physical injury exists and, under the circumstances, it is impractical for the applicant to prepare a written application without risk of such death or injury occurring."[22] The statute allows for an oral application, or an application by other electronic means, to obtain a temporary authorization for eavesdropping.[23] The authorization can last up to twenty-four hours before a standard eavesdropping warrant is required.[24] Second, the NYPD expands the type of crimes that eavesdropping can be used to investigate. The policy cites CPL § 700.05(8), which lists the type of offenses that an eavesdropping warrant can be

[19] *See* CPL Article 690.
[20] *See* CPL Article 705.
[21] CPL § 700.15(4).
[22] CPL § 700.21(1).
[23] *See* CPL § 700.21.
[24] *See* CPL § 700.21(4).

obtained for, but then the policy lists additional offenses in which the NYPD would use eavesdropping without a warrant. The NYPD's exigent circumstances policy is inconsistent with binding New York State law. Therefore, it is unlawful and unjustified. If parts of the policy that violate New York's law on eavesdropping are only meant to apply to pen registers and trap-and-trace devices, then it must be clearly stated.

The draft policy's description of access to the CALEA collection system and the data retrieved from it is vague. The policy claims that only "authorized users" will be given access to the system or its data but never describes how it is determined someone is an authorized user, who makes that determination, how that determination is monitored, or the circumstances under which a person would no longer be deemed an authorized user. Similarly, the "proper documentation" needed to be submitted to TARU to gain access to the system is not described. It is difficult, if not impossible, to determine whether the documentation required is sufficient when the requirements remain unknown. Likewise, the penalties for misuse or unauthorized access are not listed.

The policy also states that the CALEA collection system is a "closed system" and "does not reside on the NYPD computer network." However, it does not say who controls the system or which computer network the system resides on. Without this information, it cannot be determined whether that agency or company would abide by the same restrictions, including whether the data would be shared as part of immigration enforcement.

The policy also fails to set forth how supervisors of people using the CALEA collection system ensure it is being used properly. The direction to "inspect all areas containing NYPD computer systems at least once each tour and ensure that all systems are being used within NYPD guidelines" does not provide any insight to how proper review would be accomplished.

C. Cell-Site Simulators

The NYPD's draft policy on cell-site simulators is inadequate and inaccurate. An eavesdropping warrant is required for the use of a cell-site simulator, but the draft policy does not require it. Cell-site simulators are invasive, and the current search warrant statute[25] fails to provide

[25] CPL Article 690.

adequate safeguards or properly govern the use of such a device. The statute has not been updated to consider modern technology, include location tracking tools. In fact, the statute limits searches to premises, vehicles, and persons,[26] which does not include real-time tracking of individuals or their devices. Discussing the requirement for a warrant to surreptitiously attach a GPS device to a vehicle,[27] the Practice Commentaries to CPL 690.05 state "it now appears that problems based upon increased technology may call for either another change in the statutory definitions of this article, or perhaps other legislation for a new form of warrant."[28] However, no legislation has passed in the State of New York to update the search warrant statute or to add a new type of warrant that would cover real-time location tracking. As a result, cell-site simulators and related devices are better covered by the eavesdropping warrant statute.[29]

In *People v. Gordon*,[30] the Court granted suppression of a lineup because the NYPD had used a cell-site simulator without a warrant. Justice Martin Murphy found that the use of a cell-site simulator cannot be granted by a pen register and trap-and-trace order under CPL Article 705: "[I]t is improper under New York Law [Article 705.00] to authorize the obtaining of any information from a suspect's phone other tha[n] the phone numbers dialed or otherwise transmitted in outgoing and incoming calls and/or an originating phone number." *Gordon* at 547. He further stated that not only is a warrant required but the more burdensome procedures and limitations of an eavesdropping warrant under CPL Article 700 is necessary. The Court ruled:

> By its very nature…the use of a cell site simulator intrudes upon an individual's reasonable expectation of privacy, **acting as an instrument of eavesdropping** and requires a separate warrant supported by probable cause rather than a mere pen register/trap and trace order such as the one obtained in this case by the NYPD.

Gordon at 550 (citations omitted; emphasis supplied). Additionally, as discussed under the CALEA collection system policy section, the eavesdropping warrant statute has a specific procedure for when

[26] *See* CPL § 690.05(1).
[27] *See People v. Weaver*, 12 N.Y.3d 433 (2009) and *United States v. Jones*, 565 U.S. 400 (2012).
[28] Peter Preiser, *McKinney's Practice Commentary to CPL § 690.05*.
[29] CPL Article 700.
[30] 58 Misc.3d 544 (Sup. Ct., Kings Co. 2017).

there is an emergency or exigent circumstance, thus making the less restrictive policy suggested by the NYPD to be unnecessary.

It is also concerning that the NYPD consistently refers to a "probable cause order". Though an eavesdropping warrant would be the most appropriate legal process, if the NYPD is conceding at minimum that probable cause is a requirement, then there appears to be no legitimate reason not to require a search warrant. In the past, the NYPD has obtained pen register and trap-and-trace orders to justify their use of cell-site simulators. Such an order does not require a finding of probable cause but only the lower standard of "reasonable suspicion."[31] As a result, courts were not requiring probable cause, explicitly or implicitly. In addition, most judges do not have a clear understanding of what cell-site simulators are, how they work, or the problems associated with their use. Seeking a pen register or trap-and-trace order, even one based on probable cause, to justify using a cell-site simulator is a deceptive practice.

The NYPD claims that "[t]here are no known health and safety issues with cell-site simulators or the associated software." While the devices themselves may not directly impact a person's health, cell-site simulators have the capability to hinder cell phone users' ability to access emergency services and their cell service.[32] The device requires all cell phones in range, including non-target phones, to connect to it. By forcing the phones to connect to the device, instead of a legitimate cell phone tower, it interferes with the cellular service and the use of the individuals' phones.[33] Although some authorities have claimed that the devices were designed to allow 911 calls to pass through to an actual cell tower, a Canadian investigation revealed that cell-site simulators can sometimes interfere with the ability to call 911.[34] In 2018, the Harris Corporation, one of the

[31] CPL § 705.10(2).

[32] *See Government Cellphone Surveillance Catalogue*, p. 51, The Intercept, Dec. 17, 2015, available at https://theintercept.com/document/2015/12/16/government-cellphone-surveillance-catalogue/ [last accessed Feb. 12, 2021]. (warning that cell-site simulator model Stingray I/II "drains battery and raises signal strength" from phones that connect to it, and that "[i]mproper use can impact network.").

[33] Kim Zetter, *Feds Admit Stingrays Can Disrupt Cell Service of Bystanders*, Wired Magazine, Mar. 1, 2015, available at https://www.wired.com/2015/03/feds-admit-stingrays-can-disrupt-cell-service-bystanders/ [last accessed Feb. 12, 2021].

[34] Dave Seglins et al., *RCMP reveals use of secretive cellphone surveillance technology for the first time*, CBC News, Apr. 5, 2017, available at http://www.cbc.ca/news/technology/rcmp-surveillance-imsi-catcher-mdi-stingray-cellphone-1.4056750 [last accessed Feb. 12, 2021].

NYPD's vendors, admitted that its cell-site simulators may prevent anyone within range from calling 911. Senator Ron Wyden, in a letter to then U.S. Attorney General Jefferson Sessions, stated:

> Publicly-available DOJ cell-site simulator warrant applications submitted to courts after the [DOJ Policy] guidance went into effect include just a single sentence addressing disruption of the target's communications, noting that a cell-site simulator "may interrupt cellular service of phones or other cellular devices within its immediate vicinity." This statement significantly underplays both the likelihood and impact of the jamming caused by cell-site simulators.
>
> Senior officials from the Harris Corporation – the manufacturer of the cell-site simulators used most frequently by U.S. law enforcement agencies – have confirmed to my office that Harris' cell-site simulators completely disrupt the communications of targeted phones for as long as the surveillance is ongoing. According to Harris, targeted phones cannot make or receive calls, send or receive text messages, or send or receive any data over the Internet. Moreover, while the company claims its cell-site simulators include a feature that detects and permits the delivery of emergency calls to 9-1-1, its officials admitted to my office that this feature has not been independently tested as part of the Federal Communications Commission's certification process, nor were they able to confirm this feature is capable of detecting and passing-through 9-1-1 emergency communications made by people who are deaf, hard of hearing, or speech disabled using Real-Time Text technology.[35]

In other words, if people have the misfortune of being near a cell-site simulator at the time of an emergency, they may not be able to call loved ones and their attempts to call 911 may be thwarted.

Some models of cell-site simulators are capable of intercepting communications and data in transit. For example, a cell-site simulator may be able to intercept a phone call or a text message that is sent to or by a cell phone within range of the device. The draft policy states that cell-site simulators are used only for the purpose of locating individuals. It also says that: "Cell-site simulators are not used to collect the contents of any communication or any data contained on the [cellular] device itself. Cell-site simulators also do not capture emails, texts, contact lists, images or any other data from the device, nor do they provide subscriber account information (for example, an

[35] Letter from Sen. Ron Wyden to then Attorney General Jefferson Sessions, Aug. 21, 2018, available at https://www.wyden.senate.gov/imo/media/doc/08212018%20RW%20Stingray%20Jamming%20Letter%20to%20DOJ.pdf [last accessed Feb. 12, 2021]. ("urg[ing] the Department of Justice (DOJ) to be more forthright with federal courts about the disruptive nature of cell-site simulators").

account holder's name, address, or telephone number)." The policy should further clarify the NYPD approved uses for a cell-site simulator by explicitly stating that a simulator may not be used to intercept content in transit, not just content that is at rest on a device. Moreover, the policy should also state whether the cell-site simulators the NYPD possesses and/or uses are capable of intercepting content, regardless if the NYPD uses that feature. Technology and policies are ever evolving, and it is important to be transparent about existing capabilities, especially as it may relate to potentially future uses.

Simply providing the vendors, manufacturers, and models for the cell-site simulators would be an important step towards transparency and resolving the concerns about the interception of content. But, as with most of the draft policies, there is no mention of the vendors that NYPD contracts with to obtain cell-site simulators. We know from separately obtained records that the NYPD has previously contracted with the Harris Corporation,[36] now L3Harris Technologies, and more recently entered a contract with the KeyW Corporation.[37] It is unknown if the NYPD has purchased or obtained cell-site simulators from other companies. Additionally, the specific type or models of cell-site simulators the NYPD possesses or has access to has not been publicly released. The NYPD successfully fought a Freedom of Information Law Article 78 brought by the New York Civil Liberties Union, preventing model and capability information from being disclosed.[38]

D. Domain Awareness System

The NYPD's draft policy on the Domain Awareness System (DAS) fails to comply with the POST Act's mandates. In addition to the general inadequacies discussed above, the DAS draft policy is incomplete in its descriptions of how NYPD personnel access and use the technology, the data sources that are aggregated within DAS, and the safeguards—or lack thereof—to maintain the

[36] NYPD Harris Corporation contracts, obtained by the Legal Aid Society via a Freedom of Information Law request, available at https://docdro.id/Ie3i0Rc [last accessed Feb. 22, 2021].

[37] NYPD KeyW Corporation contracts, obtained by the Legal Aid Society via a Freedom of Information Law request, available at https://docdro.id/pu5W9bN [last accessed Feb. 22, 2021].

[38] *See* NYCLU v. NYPD, Index No. 100788/2016 (Sup. Ct., N.Y. Co. 2016). Transcript of December 19, 2017 hearing available at https://docdro.id/6aqydXP [last accessed Feb. 11, 2021].

accuracy, lawfulness, and privacy of the immense amount of sensitive data on New Yorkers that is aggregated by DAS.

The draft policy discloses that DAS is used by NYPD personnel in the field to "access real-time 911 information, past history of call locations, a person's NYPD arrest history and other relevant information responding officers may need when answering calls." To comply with the POST Act mandates, the NYPD must provide more detail on the immense amount of data available to its officers in the field and may not gloss over this as simply "other relevant information." Notably, the draft policy on DAS fails to include any mention of how DAS is frequently accessed and used by most, if not all, NYPD officers assigned to patrol: smart phone and tablet applications that allow NYPD personnel to access sensitive information on New Yorkers while in the field with little or no supervision.[39] Further, the policy fails to disclose that officers use DAS smart phone and tablet applications to conduct routine records searches on New Yorkers during traffic stops and investigative encounters, pulling up "snapshots" that compile sensitive data of the person being searched, including those with no arrest record.[40]

Based on information obtained through discovery in civil and criminal litigation, the data in individual DAS "snapshots" or "Real Time Person Files" may include photographs (including photographs gathered from social media), date of birth, height, weight, race, hair color, eye color, complexion, tattoos and body markings, current and past addresses, phone numbers, current and past vehicles, people with whom the subject is associated, among other information. This information is kept in NYPD databases and aggregated by DAS regardless of whether the person has a pending criminal investigation, case against them, or criminal record. Further, DAS "snapshots" and "Real Time Person Files" of individuals contain information on suspected gang affiliation, warrants, i-cards, and arrest records—even when the warrants or i-cards have been resolved and/or the charges

[39] Based on information obtained through discovery in civil and criminal litigation. *See, e.g., Belle v. City of New York*, CIV 2673-VEC (S.D.N.Y.).
[40] *Id.*

relating to arrest records have been dismissed and sealed.[41] The DAS draft policy completely fails to address the existence of this data, much less the policies and practices used to ensure the lawfulness and accuracy of this sensitive data available to thousands of officers in the field.

Further, the draft policy mentions only a few sources of its data—including CCTV, LPRs, and ShotSpotter, that are aggregated by DAS, failing to disclose the many other streams of data that DAS aggregates. While each of these absences is concerning, the lack of transparency surrounding the sources of the data that DAS aggregates on individuals—indeed, how individuals become the subject of a DAS "snapshot" or "Real Time Person File"—is particularly troubling. In order to comply with the POST Act's mandates, the NYPD must disclose this critical information regarding data sources—from both governmental and private sources—and the criteria for individuals whom DAS aggregates data about in the form of "snapshots" and "Real Time Person Files."

Through DAS, tens of thousands of NYPD personnel and vendors have access—often by smart phone or tablet—to immense amounts of sensitive information on individual New Yorkers. Because of this, issues concerning oversight, auditing, training, legal compliance, and disparate impact are of particular concern. However, these areas of the DAS policy are severely lacking. As discussed above in the general comments, the DAS policy, like many other NYPD draft policies, contains meaningless boilerplate language, vague statements on accountability and compliance that amount to "trust us", and gaping omissions regarding its disclosure on how the technology is used by NYPD personnel. For these reasons, NYPD has failed to meet its obligations under the POST Act regarding the Domain Awareness System.

E. Data Analysis Tools

The NYPD's draft policy on Data Analysis Tools is incredibly sparse, so much so that it cannot possibly fulfill the POST Act's mandate that the NYPD adequately describe the capabilities of its surveillance tools. Only a few facts can be gleaned from what the NYPD has proposed. First,

[41] *Id.*; *See also R.C. v. City of New York*, No. 153739/2018 (N.Y. Sup. Ct., 2018) (challenging the NYPD's practice of illegally using and sharing information from sealed arrest records in defiance of long-standing privacy laws that protect privacy and the presumption of innocence).

that it possesses a generic suite of data analysis tools that use artificial intelligence and machine learning. Second, that the NYPD compiles "structured" and "unstructured" datasets, generically described as computer-readable collections of data. And, third, that the generic suite of data analysis tools is used to identify potential "connections" between otherwise isolated datasets.

That is the sum of what the NYPD has chosen to disclose in its draft policy on data analysis tools. The draft policy provides absolutely no information on the kinds of data that are used to create structured and unstructured datasets, other than they may contain "audio, video, location, and similar information," painting the picture so broadly that it ceases to have meaning. It provides no information by which one could distinguish between what the NYPD considers as a "structured" or "unstructured" dataset and why such a distinction might be meaningful. It provides no information on what constitutes a "connection" between datasets and how any such connection could prove useful in a law enforcement context. The draft policy flatly states that no biometric data is compiled within these datasets, but that contention beggars belief; one would think that, at the very least, fingerprint data would be included in either a structured or unstructured dataset that is accessible to users of the data analysis tools. The draft policy says nothing about how artificial intelligence and machine learning is used by "some" data analysis tools, such that those capacities are either deeply embedded within those tools or, alternatively, that they are only somewhat implicated. Indeed, the draft policy fails to name a single specific data analysis tool that is used by the NYPD. The draft policy cannot adequately describe the capabilities of the NYPD's data analysis tools when it refers to them in the most generic, unadorned way imaginable.

One piece of surveillance technology that may fall under this rubric is the NYPD's "Patternizr" tool, which is used for predictive policing purposes and highlights criminal activity across police precincts and command jurisdictions. The NYPD has used this tool since 2016,[42] even though it raises troubling issues of implicit, explicit, and actuarial racial bias that are embedded in

[42] Alex Chohlas-Wood & E. S. Levine, *A Recommendation Engine to Aid in Identifying Crime Patterns*, 49 INFORMS J. APPLIED ANALYTICS 154, Feb. 11, 2019, available at https://doi.org/10.1287/inte.2019.0985 [last accessed Feb. 23, 2021].

the algorithms it relies upon.[43] Patternizr could also fall prey to simple human error; that is, if data are entered incorrectly into a given dataset and said dataset is used for predictive policing purposes, it could lead to completely undue surveillance, prosecution, and conviction of a person who has committed no crime or a less serious crime than the one which he is accused of committing. The use of Patternizr also raises constitutional concerns. As the ACLU and a coalition of other civil liberties groups have argued:

> The Fourth Amendment forbids police from stopping someone without reasonable suspicion – a specific, individualized determination that is more than just a hunch. Computer-driven hunches are no exception to this rule, and a computer's judgment is never a further reason (beyond the articulable facts that intelligibly caused that judgment) for a stop, search, or arrest. Similarly, predictive policing must not be allowed to erode rights of due process and equal protection. Systems that manufacture unexplained "threat" assessments have no valid place in constitutional policing.[44]

The draft policy purports that data analysis tools must be used in a way that comports with the civil rights granted by the Federal and State Constitutions, but there is little to no way to determine that such is the case where the NYPD has failed to provide a whit of truly substantive information as to what actually constitutes data analysis tools. And, as the quotation above argues, it is likely that the NYPD's use of data analysis tools – at least in the realm of predictive policing - runs afoul of the Federal and State Constitutions' protections against unreasonable searches and seizures. At bottom, this draft policy is woefully inadequate, as it provides the public with no useful information and should be re-drafted to identify, with a great deal more particularity, what precisely constitutes a data analysis tool and how such tools are used.

F. Digital Fingerprint Scanning Devices

The draft policy on the use of Digital Fingerprint Devices suffers from the general inadequacies detailed in the beginning of this letter. It fails to fully detail retention policies specific

[43] *See* Molly Griffard, *A Bias-Free Predictive Policing Tool?: An Evaluation of the NYPD's Patternizr*, 47 Fordham Urb. L.J. 43, 2019, available online at https://ir.lawnet.fordham.edu/ulj/vol47/iss1/2/ [last accessed Feb. 23, 2021].

[44] American Civil Liberties Union & 16 Civil Rights, Privacy, Racial Justice & Tech. Orgs., *Predictive Policing Today: A Shared Statement of Civil Rights Concerns*, Aug. 31, 2016, available at https://www.aclu.org/other/statement-concern-about-predictive-policing-aclu-and-16-civil-rights-privacy-racial-justice [last accessed Feb. 17, 2021].

to this technology, how long data is retained and where, specifics regarding training, and general security protocols for access by authorized users or external entities.

The draft policy omits any information regarding the Mobile Fingerprint Identification Device. These devices are provided to officers in the field, and their use is memorialized in Operations Order 39, issued on September 9, 2010. This technology falls squarely within the purview of the POST Act and a policy must be promulgated related to its use.

G. Digital Forensics Access Tools

The NYPD's draft policy on Digital Forensics Access Tools fails to meet the statutory requirements, insofar as it insufficiently details the capabilities of the digital forensic access tools it uses and misrepresents the capacity of such tools to extract digital information from the "cloud," as opposed to just information included on the seized electronic device. It also fails to sufficiently explain how the NYPD manages to use its digital forensics access tools in a manner that comports with the Fourth Amendment's requirement that searches made pursuant to a search warrant be limited in breadth and be particularized with regard to evidence that is properly the subject of an authorized search. It further fails to state how the use of these relatively novel forensic tools results in examinations that are conducted in a forensically sound manner (i.e., without introducing extraneous data into the seized device during the course of an examination).

The draft policy does not state which vendors supply it with the hardware and software that the NYPD includes under the umbrella of "digital forensics access tools." The NYPD uses at least two vendors to supply it with such tools: Cellebrite, an Israeli based digital forensics services provider, and Grayshift, Inc., an American provider of similar services. The draft policy does not supply any information as to how these vendors were chosen, the use cases for selecting one provider over another in any given situation, and does not detail why two separate providers are necessary to provide the NYPD with the same functionality. Along the same line, the draft policy fails to even generically describe the capabilities of each vendor, beyond stating that the tools that the NYPD uses allows them to "extract" and "process" information derived from a seized electronic device. Indeed, any member of the public likely has little idea of what it means to perform a forensic extraction or analysis of an electronic device and what processing may need to be performed on the extracted data in order to use it in a criminal proceeding. The draft policy further fails to mention what types of electronic devices could be subject to forensic extraction or analysis using the tools provided by these vendors (i.e., which tool can perform forensic analyses/extractions on which types of electronic devices). It also fails to detail how the tools it uses creates a proper chain of custody for the information seized from any electronic device.

The draft policy also states that digital information can only be extracted from a seized electronic device and from nowhere else. However, Cellebrite offers a product called "UFED Cloud Analyzer" that is capable of extracting data from the "cloud," instead of the seized device.[45] Given the NYPD's longstanding contracts with the NYPD/DANY, they are likely aware of this functionality, if they do not actively use it in the course of criminal investigations. The fact that this capacity exists means that the NYPD must include it in the policy it ultimately issues for this policy to conform with the POST Act's requirements.

Turning to constitutional concerns, the draft policy only generically refers to conducting investigations using digital forensics access tools in a manner that comports with the Federal and State Constitutions. However, time and again, NYPD officers perform "general," rummaging searches through the entirety of an electronic device and/or account, in violation of the requirement that any search be narrowly tailored to the crime for which the evidence is being sought and that the search warrant provide necessary particularity in authorizing the parameters of the search. The NYPD's policy on digital forensic access tools should describe the ways in which NYPD investigators ensure that their analyses comport with these essential constitutional requirements.

Finally, as any digital forensic investigator knows, one must take affirmative steps to prevent the introduction of extraneous data into the seized device that one is forensically analyzing. This is crucial to maintaining the integrity of any evidence seized using digital forensics tools, yet the draft policy is completely silent on the account. The NYPD's policy should – at least generically – speak to the efforts it makes to conduct forensically sound analyses or extractions. As it stands now, no

[45] *See* Cellebrite UFED Cloud Analyzer, https://www.cellebrite.com/en/ufed-cloud-analyzer-5/ [last accessed Feb. 17, 2021].

member of the public could be assured that digital evidence seized and used against them in a criminal proceeding was obtained in a forensically sound manner by reading the draft policy.

H. Drone Detection Systems

The draft Impact and Use Policy explains that NYPD drone detection systems are capable of "process[ing]" audio signals, geo-location data, and video and still images. As such, drone detection systems "implicate a variety of federal and state laws relating to surveillance and the capturing of electronic communications." The policy states that drone detection technology is "guided by reviews conducted by the NYPD Legal Bureau to ensure such usage is in compliance with state laws related to eavesdropping as well as federal laws such as the Pen/Trap-and-Trace Device Statute (18 U.S.C. §§ 3121-3127) and the Wiretapping Act (18 U.S.C. §§ 2510 *et. seq*)." The policy also references advisories published by the federal Department of Justice, Department of Homeland Security, and the Federal Aviation Administration. Finally, the policy explains that if the use of drone detection systems "are not exempt under the aforementioned statutes, or if no exceptions to the warrant requirement exist, pen register or trap and trace orders can be obtained..."

Although the policy acknowledges the implications of utilizing a drone detections system that can intercept electronic communications, it fails to explain the legal basis NYPD is using to deploy and use these systems. The policy references "reviews conducted by the NYPD Legal Bureau" but does not include or summarize the substance of these reviews. It omits an explanation of how these reviews analyze the applicable state laws like CPL Art. 700 and Art. 705 or the referenced federal statutes. Similarly, there is no explanation of how the "advisories" published by the federal agencies affect how and when NYPD is legally entitled to deploy drone detection systems. Lastly, the policy fails to discuss whether a pen register or trap-and-trace order is the appropriate legal process for intercepting electronic communications. In 1988, New York updated its wiretapping law to apply "beyond devices that transmit the human voice to transmissions of words, data and signals sent by fax machines, computers, pen registers, trap and trace devices, and photo-optical systems, etc."[46] The policy's reliance on pen register and trap-and-trace orders to permit

[46] *See* Preiser, *McKinney Practice Commentary to CPL § 700.05*.

drone detections systems does not consider the strong privacy grounds underlying New York's eavesdropping statutes and the stringent requirements they contain.[47]

I. Facial Recognition

The NYPD's draft policy on its facial recognition surveillance technology fails to meet the POST Act's mandates, insofar as it fails to adequately address the capabilities of such technology, misrepresents whether its use of facial recognition technology relies on AI and/or machine learning and whether its potential candidate images are obtained from "a controlled and limited group of photographs already within lawful possession of the NYPD," and fails to adequately address the documented disparate impact that the use of facial recognition technology has on minority communities.

First, the NYPD's description of the capabilities of its facial recognition technology lacks crucial substance, bearing directly on the NYPD's ability to manipulate probe images until its facial recognition software delivers the results that the NYPD needs. Probe images or probe photos are "photos of unknown individuals submitted for search against a police or driver license database."[48] The NYPD uses DataWorks Plus's FACE Plus Case Management ("DataWorks") as its facial recognition software platform. DataWorks allows for substantial manipulation of probe images, allowing NYPD officers to substantially transform the probe image into something unrecognizable from its original form. For instance, DataWorks allows the NYPD to take two-dimensional probe images and transform them into three-dimensional models, each of which comprises the original probe image and the "result" image (i.e., the image that is supposed to be a purported match). DataWorks' "pose correction tool," used in conjunction with a generated three-dimensional model allows for the NYPD to "search facial images that were once unsearchable." This is but one example of how DataWorks allows the NYPD to manipulate probe images; the software comes replete with an arsenal of tools, much like those provided in Adobe's Photoshop software, that allow NYPD

[47] *See People v. Bialostok*, 80 N.Y.2d 738, 745 (1993) (recognizing "the broad legislative intent of article 700 to safeguard individual privacy").

[48] Clare Garvie, *Garbage In, Garbage Out – Face Recognition on Flawed Data*, The Georgetown Law Center on Privacy & Technology, May 16, 2019, available at https://www.flawedfacedata.com [last accessed Feb. 17, 2021].

officers to change the sharpness, contrast, brightness, color saturation, RGB balance, and light normalization for a given probe image. It follows naturally that NYPD officers are not comparing pristine, "virgin" probe images to databases to generate reliable matches. Instead, DataWorks allows the NYPD to generate facial recognition matches that would otherwise not exist. In fact, NYPD officers have even used celebrity "look-a-likes" to generate purported facial recognition matches, which are use cases that are not blessed by DataWorks.[49]

Second, the draft policy states that the NYPD's facial recognition technology does not rely on, *inter alia*, machine learning. This is false. DataWorks uses algorithmic search engines derived by NEC and Cognitec to perform its tasks and both the NEC and Cognitec search engines rely on deep learning technologies.[50] "Deep learning" is simply a technique for implementing machine learning to a task by using neural networks.

Third, the draft policy flatly states that potential candidate images are derived solely from a controlled and limited database of images that the NYPD "lawfully obtained."[51] The NYPD has previously claimed that the database of images used for facial recognition has only contained arrest photos.[52] The policy does not limit the photos to arrest photos, fails to mention the sources of the

[49] *See* Drew Harwell, *Police have used celebrity look-alikes, distorted images to boost facial-recognition results, research finds*, The Washington Post, May 16, 2019, available at https://www.washingtonpost.com/technology/2019/05/16/police-have-used-celebrity-lookalikes-distorted-images-boost-facial-recognition-results-research-finds/ [last accessed Feb. 17, 2021]; Clare Garvie, *Garbage In, Garbage Out – Face Recognition on Flawed Data*, The Georgetown Law Center on Privacy & Technology, May 16, 2019, available at https://www.flawedfacedata.com [last accessed Feb. 17, 2021].

[50] *See* NEC Corporation, *NEC technology recognizes people based on partial images*, Feb. 8, 2019, available at https://www.nec.com/en/press/201902/global_20190208_01.html [last accessed Feb. 17, 2021]; Cognitec Systems GmbH, *FaceVACS Engine enables clients to develop new face recognition and facial image analysis applications*, available at https://www.cognitec.com/facevacs-technology.html [last accessed Feb. 17, 2021].

[51] This is deeply questionable. While NYPD policy mandates that probe images should only be run against such a controlled and limited database, the New York Post reported roughly a year ago that NYPD officers were using the controversial Clearview AI software program to conduct thousands of facial recognition searches outside of approved NYPD policy. *See* Craig Warner, *Rogue NYPD cops are using facial recognition app Clearview*, The New York Post, Jan. 23, 2020, available at https://nypost.com/2020/01/23/rogue-nypd-cops-are-using-sketchy-facial-recognition-app-clearview/ [last accessed Feb. 17, 2021].

[52] James O'Neill, *How Facial Recognition Makes You Safer*, The New York Times, June 9, 2019, available at https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html [last accessed Feb. 24, 2021] ("A database consisting solely of arrest photos is then searched as the sole source of potential candidates — not photos from the Department of Motor Vehicles, Facebook, traffic cameras or the myriad streams of close-circuit TV video from around the city.").

images, or how the NYPD's procurement of the images was lawful. This is particularly concerning because there has been evidence to suggest that some of the candidate photos may also be derived from social media images.[53] The policy seemingly intentionally obscures the source of the photos, suggesting that the images are not limited to arrest photos – as previously claimed – and that the NYPD considers images acquired from their social media monitoring to be "lawfully obtained."

The policy also fails to provide any guidance for how a possible facial recognition match may be used, beyond that it "serves as a lead" and that it cannot be the sole basis for an arrest. This leaves an unjustified level of discretion to detectives and officers, most of whom do not have any understanding of the concerns with facial recognition. As a result, the NYPD has left open whether or not possible facial recognition matches can be used to justify the stop of people on the street, pulling over their vehicles, appearing at their work, etc. While an arrest is a traumatic experience, these "lesser" interactions with law enforcement can also be traumatic and disruptive. They also may be unlawful, if justified by only a possible facial recognition match.[54]

Finally, the draft policy blithely references a non-specified federal study that allegedly shows that the disparate effects that the use of facial recognition technology has on non-white men can be corrected through the intervention of human reviewers. This is insufficient to meet the POST Act's mandate that a Surveillance Policy affirmatively detail said disparate impacts where such exist. The disparate effects of facial recognition technology have been well-documented. For example, a 2018 MIT Media Lab study discovered that facial recognition technology algorithms designed by Microsoft, IBM, and a company named "Face++" had error rates of up to 35% or higher when attempting to identify dark-skinned women; those same error rates dropped to less than 1% when attempting to identify white men.[55] The ACLU's test of Amazon's facial recognition software misidentified 28 U.S. congresspersons as criminals; congresspersons of color were

[53] Mike Hayes, *The NYPD May Be Secretly Using Facebook Photos In Its Facial Recognition Searches*, The Huffington Post, Feb. 14, 2020, available at https://www.huffpost.com/entry/nypd-facial-recognition-facebook-social-media_n_5e46da8bc5b64433c615d9a1 [last accessed Feb. 23, 2021].

[54] *See generally People v. DeBour*, 40 N.Y.2d 210 (1976).

[55] *See* Larry Hardesty, *Study finds gender and skin-type bias in commercial artificial-intelligence systems*, MIT News, Feb. 11, 2018, available at https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212 [last accessed Feb. 17, 2021].

disproportionately identified as criminals.[56] The New York Times found that the NYPD's use of juvenile mugshots as a dataset for "virtual lineups" demonstrated a higher risk of misidentification when facial recognition technology is applied to "young" faces.[57] And recent research from the University of Colorado found that non-binary persons are consistently misclassified by facial recognition technology.[58]

With all of that said, the policy should also meaningfully reckon with the fact that people of color are more likely to be disproportionately affected by the NYPD's use of facial recognition technology because people of color are disproportionately misidentified, arrested, and put through the rigors of the criminal justice system.[59] The draft policy's attempt to hand wave away systemic and troubling disparities of the effect of facial recognition technology is both troubling and inadequate to fulfill the NYPD's obligations under the POST Act.

J. Internet Attribution Management Infrastructure

The Internet Attribution Management Infrastructure draft policy is sparse on details and lacks sufficient restrictions. The policy states that the Infrastructure "may be used in any situation the supervisory personnel responsible for oversight deems appropriate." It further states that "[t]he underlying facts are considered on a case-by-case basis prior to the utilization of the technology, including the legitimate law enforcement purpose to utilize the technology in a given circumstance." These restrictions are not restrictions at all. There are no limitations on the type of case or investigation for when the Infrastructure can be used. There is no definition or even guidelines included to determine what qualifies as a "legitimate law enforcement purpose".

[56] *See* Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, The American Civil Liberties Union, July 26, 2018, available at https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [last accessed Feb. 17, 2021].

[57] *See* Joseph Goldstein & Ali Watkins, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database.*, The New York Times, Aug. 1, 2019, available at https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html [last accessed Feb. 17, 2021].

[58] *See* Lisa Marshall, *Facial recognition software has a gender problem*, CU Boulder Today, Oct. 8, 2019, available at https://www.colorado.edu/today/2019/10/08/facial-recognition-software-has-gender-problem [last accessed Feb. 17, 2021].

[59] *See, e.g.*, Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, The New York Times, Dec. 29, 2020, available at https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html [last accessed Feb. 17, 2021].

The permission of unnamed unidentified "supervisory personnel" is the sole gatekeeper for this technology, and the supervisory personnel are not given any guidance or requirements in how to determine which requests to approve. Additionally, there is no paperwork listed that would document a request, its approval or disapproval, or the reasons for why permission was granted or denied. The draft policy allows for an arbitrary decision by a supervisor of unspecified rank.

The policy lists equipment utilized as part of the Internet Attribution Management Infrastructure, including virtual private networks (VPNs). It does not include the vendor information for the VPNs, if the NYPD has set up its own VPNs, or if they are using a mix of third-party vendors and internally created VPNs. The importance of such distinction here is that not all VPNs handle private data equally. For example, the policy should include if logs are kept of the activity conducted while using a VPN, how long those logs are kept, and who possesses or has access to the logs (i.e. the NYPD or a third-party?). Similarly, there are no mentions of whether members of the NYPD are permitted to use Tor[60] or I2P,[61] to access websites that are not technically private but require either of those two applications/networks to access them.

Furthermore, there are no prohibitions on violating the rules or policies of the sites and platforms that members of the NYPD are visiting or using. Relatedly, there is no guidance or limitation on how and when personnel may use false information or identities.[62] Specifically, there are nothing in the policy that prevents officers from falsely using the identity of a real person, without that person's consent or knowledge.[63]

K. Iris Recognition

The Iris Recognition draft policy is inadequate to address the requirements of the POST act. Since its inception in 2010, iris scans have been the subject of the precise criticisms the POST act was designed to address. The draft policy ignores these long-standing objections to the manner iris

[60] *Tor Project | Anonymity Online*, available at https://www.torproject.org/ [last accessed Feb. 15, 2021].

[61] *I2P Anonymous Network*, available at https://geti2p.net/ [last accessed Feb. 15, 2021].

[62] *See generally Information for Law Enforcement Authorities: Authenticity Policy*, Facebook, available at https://www.facebook.com/safety/groups/law/guidelines/ [last accessed Feb. 15, 2021].

[63] *See generally* Chris Hamby, *Government Set Up a Fake Facebook Page in this Woman's Name*, BuzzFeed News, Oct. 6, 2014, available at https://www.buzzfeednews.com/article/chrishamby/government-says-federal-agents-can-impersonate-woman-online [last accessed Feb. 15, 2021].

scans are administered. In particular, the policy doubles down on the lack of a legal foundation for the NYPD's use of iris scans. The NYPD determined that no statutory authorization was required to use the technology and did not engage in any discourse with stakeholders or the public.[64] They continue to rely on this assertion in their draft policy, without citing any legal precedent or authority from their own Legal Department or otherwise. They have neither requested nor obtained any legal opinion from an objective party outside of the NYPD.

As discussed more generally above, this policy also fails to address the specific training provided to officers on use of the technology. The policy makes clear that, "in order for an iris image to be taken, arrestees must provide their consent" and that "failure or inability to capture an iris image will not materially delay arraignment." The policy fails to detail how this information is communicated to arrestees. It also fails to outline what training officers receive on how to proceed when consent is not given. This is particularly troubling considering the continued confusion regarding the voluntary nature of the scan, and the regular practice of the NYPD to delay arraignment of an individual asserting the right not to consent.[65]

The draft policy also relies on the assertion that iris scanning ensures that arrestees are being arraigned in connection to the correct case. They further continue to justify the implementation of this procedure based on a mere six incidents of alleged misidentifications occurring prior to 2010. The draft policy makes the baseless assertion that "since the implementation of the iris recognition program, [there have been] no such incidents." The policy provides no statistics, reports, or the

[64] Ray Rivera & Al Baker, *New York City Police Photograph Irises of Suspects*, The New York Times, Nov. 15, 2010, available at https://www.nytimes.com/2010/11/16/nyregion/16retinas.html [last accessed Feb. 22, 2021] ("'It's really distressing that the Police Department is once again undertaking a new regime of personal data collection without any public discourse,' said Donna Lieberman, the executive director of the New York Civil Liberties Union, 'and we don't know the reason for it, whether this is a necessary program, whether it's effective to address the concerns that it's designed to address, and whether in this day and age it's even cost-effective, not to mention whether there are any protections in place against the misuse of the data that's collected.'").

[65] Colin Moynihan, *Some Who Decline an Optional Iris Photo Are Kept Longer in Jail, Critics Say*, Feb. 12, 2012, available at https://www.nytimes.com/2012/02/13/nyregion/new-objections-to-nypds-iris-photographing-program.html [last accessed Feb. 22, 2021] ("Steven Banks, the attorney in chief for the Legal Aid Society, said that when the program began, clients who did not submit to the photographs were processed normally. That changed recently, he said, and the police have delayed the arraignment of some Legal Aid Society clients who declined iris photographs."); *See also Leibowitz v. City of New York, et al.*, 12 CIV 8982 (JSR).

results of auditing, to back up this claim. To properly comply with the requirement of the POST act, specific audits regarding the results and use of the technology must be outlined and implemented.

L. License Plate Readers (LPR)

The NYPD's draft policy on its use of license plate readers (LPRs) drastically minimizes the capabilities of this surveillance technology and fails to mention the NYPD's partnership with Vigilant Solutions ("Vigilant"), a vendor that provides the NYPD with a disturbing amount of surveillance capability. A more fulsome description of the NYPD's capability to track individuals through its partnership with Vigilant is necessary to bring the draft policy in compliance with the POST Act's requirement that the capabilities of a given surveillance technology be adequately described.

The NYPD contracted with Vigilant as a vendor to supply it with LPR technology in 2014; that contract has been extended every two years since 2014 and is still in effect. Specifically, the NYPD's Real Time Crime Center has purchased a data subscription to Vigilant's Law Enforcement Archival and Reporting Network ("LEARN"). Due to this partnership, the NYPD's capability to surveil drivers is greatly enhanced beyond the bare-boned description given in the draft policy. First, this partnership provides the NYPD with access to "the nation's largest repository of collected Private LPR Data"; this collection of private LPR data is comprised of over 2.2. billion LPR data records, growing at a rate of around 100 million new LPR records per month. The private LPR data is shared with law enforcement through the LEARN Database (as opposed to a mere "administrative database"). Vigilant leverages its partnerships with non-law enforcement clients to obtain private LPR data and then provides such data to law enforcement agencies that contract with it. This private LPR data is derived from locations where vehicles remain or re-appear for extended periods of time; these locations include residential areas, retail areas, and business office complexes with large parking lots. Vigilant states that the provision of this data to law enforcement agencies allows the latter to "have the additional benefit of *immediate intervention* of an occupied vehicle of interest." Vigilant further states that LEARN allows law enforcement to "quickly conduct[] historical and *real-time* queries" against search parameters. LEARN's "geo-zoning" functionality allows law enforcement to receive the nearest physical address and nearest intersection to a surveilled vehicle which, it states, “is helpful for situations requiring *immediate* dispatch.” In fact, Vigilant states that, on average, it only takes a fraction of a minute for private LPR data to become available within LEARN.

Vigilant also provides a “stakeout” feature that allows NYPD investigators to surveil vehicle visits within a user-drawn “geo-fence.” More disturbingly, the stakeout feature can be used in conjunction with “associate analysis” that provides NYPD investigators with the ability to determine which other vehicles are commonly seen around a particular vehicle, where the “common” vehicles may be criminal suspects, political or religious associates, or even family members. Vigilant, through LEARN, also offers the NYPD the ability to determine the most likely location for a given vehicle based on a statistical analysis. The data used for that analysis include, among other factors, whether a given location where a vehicle was seen is a “public or private area.” Vigilant advertises its services by announcing that through “transgressing the boundaries of locally harvested data, LEARN provides a broader scope of investigative lead sources” and that “the RTCC will benefit by adding the investigative tools only available in LEARN and having a true ‘force multiplier’ by gaining access to private data being acquired daily in the field.”

What is clear from Vigilant’s partnership with the NYPD is that the NYPD’s surveillance capabilities through the use of LPR technology are considerably broader and deeper than what it describes in a bareboned fashion in the draft policy. Instead, the NYPD actively leverages privately acquired data, sweeping in the locations and movements of citizens unsuspected of any criminal activity derived, in some instances, of scans taken in non-public areas, through its use of said technology. The NYPD’s License Plate Reader Policy must be revised to account for the full capabilities of this technology.

M. Mobile X-Ray Technology

The draft policy regarding use of Mobile X-Ray inadequately addresses nearly every mandate of the POST Act. It provides only vague information regarding the capabilities of the device, who or what kind of authorization is necessary, how long images are retained, the interplay of privacy rights and release of the information to third party entities, protocols for auditing use of the devices, and any health and safety information.

Rather than describe the actual capabilities of the device, the policy provides only a cursory description of its use and instead details what it does not do. The policy also asserts that the device's undisclosed manufacturer ensures compliance with safety standards, and functions within well-established health guidelines, but fails to provide any user manuals, reports, or statistics to back up this claim. Auditing and safety are discussed only regarding the devices themselves, but not their actual use by NYPD personnel.

The draft policy contains the oft repeated and baseless assertion that use of Mobile X-Ray Devices does not require court authorization because it is employed in a manner that comports with the special needs exception to the warrant requirement. The policy provides no legal precedent or opinion to back up this claim. This assertion belies a quintessential misunderstanding of the special needs exception, which requires that the search is conducted for purposes beyond the normal needs of law enforcement.[66] The policy itself lists examples of situations in which use of the device is authorized that by the furthest stretch, cannot be considered anything but traditional law enforcement activities.

The policy must provide transparency regarding authorized users, their training, and the decision-making process prior to utilizing the device. It is vague in all these regards, referring repeatedly to "other authorized users" without further information. The policy allows for the NYPD to turn over retained imaged to the community and media without articulating the requirements for doing so, the justifications, and how these approvals balance legitimate privacy rights.

N. ShotSpotter

The New York City Police Department's ShotSpotter draft Impact & Use Policy states that "ShotSpotter devices are not and cannot be used to covertly listen to conversations, street-noise, or any non-gunfire acoustic data." Furthermore, the policy states that ShotSpotter "does not use artificial intelligence, machine learning, or biometric measurement technology." Based on publicly available information, including representations made by ShotSpotter on their corporate website, these statements misstate or unduly minimize the capabilities of ShotSpotter and the surveillance

[66] *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985).

aspects of the system. As the policy fails to correctly explain the capabilities of ShotSpotter, the policy should be revised to reflect the actual operation of the system.

First, contrary to the statement in the policy, ShotSpotter is capable of covertly recording conversations, street-noise, and non-gunfire noises. In at least two instances, ShotSpotter has recorded conversations that have subsequently been provided to law enforcement.[67] In 2019, the Policing Project at New York University Law School conducted a privacy audit of ShotSpotter. The audit concluded that although the risk of voice surveillance was "extremely low in practice" it was "surely possible that ShotSpotter sensors will, on occasions, capture some intelligible voice audio related to a gunfire incident."[68] Additionally, ShotSpotter's privacy policy acknowledges the conclusions of the Policing Project and explains the measure taken by ShotSpotter to minimize the recording of voice audio.[69] The policy fails to accurately describe the recording capabilities of ShotSpotter and, as a result, does not include any discussion of how NYPD will work to prevent the recording of conversations.

Second, the draft policy incorrectly states that ShotSpotter does not use artificial intelligence or machine learning. While the term "artificial intelligence" has no universally accepted definition, it is generally agreed that these systems "make decisions which normally require [a] human level of expertise and help people anticipate problems or deal with issues as they come up."[70] The closely related concept of machine learning refers to "algorithms [that] use statistics to find patterns in

[67] *See* CBS San Francisco, *Oakland's Shotspotter Equipment Records Voice Conversations*, May 21, 2014, available at https://sanfrancisco.cbslocal.com/2014/05/21/shooting-crime-privacy-tech-oaklands-shotspotter-equipment-records-voice-conversations/ [last accessed Feb. 3, 2021]; Erica Goode, *Shots Fired, Pinpointed and Argued Over*, New York Times, May 28, 2012, available at https://www.nytimes.com/2012/05/29/us/shots-heard-pinpointed-and-argued-over.html [last accessed Feb. 3, 2021].
[68] Policing Project at NYU Law, *Privacy Audit & Assessment of ShotSpotter Inc.'s Gunshot Detection Technology*, July 2019, available at https://www.policingproject.org/s/Privacy-Audit-and-Assessment-of-Shotspotter-Flex.pdf [last accessed Feb. 3, 2021].
[69] ShotSpotter, *Privacy Policy: Community Privacy Protections*, July 2019, available at https://www.shotspotter.com/privacy-policy/ [last accessed Feb. 19, 2021].
[70] *See* Darrell M. West, *What is Artificial Intelligence?*, The Brookings Institution, Oct. 4, 2018, available at https://www.brookings.edu/research/what-is-artificial-intelligence/ [last accessed Feb. 15, 2021].

massive amounts of data."[71] Contrary to the statement in the draft policy, ShotSpotter uses artificial intelligence and machine learning to train its system to recognize the sound of gunfire.[72] In fact, ShotSpotter's website includes a section on "Technology" which states the following under the heading "Artificial Intelligence and Machine Learning":

> Investments in algorithms, artificial intelligence, machine learning and more recently deep learning have enabled us to continuously improve our ability to accurately classify gunshots. With more than 15 million incidents reviewed to date, ShotSpotter is in a unique position to feed this trove of data into our system for increasingly smarter and more precise results.

The draft policy incorrectly states that ShotSpotter does not use artificial intelligence or machine learning. Based on ShotSpotter's own website, this is incorrect. The draft statement needs to address the use of artificial intelligence and machine learning by ShotSpotter.

The policy also fails to discuss the proper legal authority for utilizing ShotSpotter. The policy states that ShotSpotter use must be consistent with the federal and state constitutions and any applicable statutes. However, the policy further asserts that "[c]ourt authorization is not necessary" and that "[g]unfire detection sensors process acoustic data that is audible in open, public locations that do not enjoy a reasonable expectation of privacy." As discussed above, the policy falsely claims that ShotSpotter cannot record human conversations. However, as the system is capable of recording conversations and has done so in the past, it should be considering an eavesdropping device, as defined in CPL § 700.05, because it has the capacity to "mechanical[ly] overhear[] . . . conversation." As an eavesdropping device, capable of intruding into the private conversations of pedestrians on the street, ShotSpotter is subject to the eavesdropping warrant provisions of CPL § 700. As such, law enforcement officials should be required to obtain an eavesdropping warrant, based upon probable cause, before installing or using ShotSpotter.[73]

[71] *See* Karen Hao, *What is machine learning?*, MIT Technology Review, Nov. 17, 2018, available at https://www.technologyreview.com/2018/11/17/103781/what-is-machine-learning-we-drew-you-another-flowchart/ [last accessed Feb. 15, 2021].

[72] *See ShotSpotter Respond FAQ*, Dec. 2020, available at https://www.shotspotter.com/wp-content/uploads/2020/12/ShotSpotter-Respond-FAQ-Dec-2020.pdf [last accessed Feb. 15, 2021]. ("This data is used to locate the incident and is then filtered by sophisticated machine algorithms to classify the event as a potential gunshot.")

[73] *See* CPL § 700.15.

As the New York Court of Appeals has explained, CPL § 700 "requires scrupulous compliance[.]"[74] Indeed, the Court of Appeals has "consistently recognized the 'insidiousness of electronic surveillance' . . . and . . . that '[the] interpretation of article 700 must be sensitive to the constitutional guarantees against search and seizure that the statute seeks to protect."[75] Furthermore, the fact that ShotSpotter is intended to "hear" gunshots and not conversation is irrelevant as to whether an eavesdropping warrant is required. The Court of Appeals has found that even though "no unauthorized eavesdropping may have occurred is beside the point, because it is the potential for abuse that is the focus of analysis."[76] In *Bialostok*, the "audio" function that made the device at issue subject to CPL 700 was "off" and did not record any conversation, but the court nonetheless found that the issue was "not the reasonableness of the search but statutory compliance."[77] There is a significant potential for abuse of the ShotSpotter device as an eavesdropping device.

O. Situational Awareness Cameras

The draft policy on Situational Awareness Cameras inadequately addresses the POST Act requirements on training, authorization, and the myriad legal implications of their use. As with many of the other policies, the policy claims a blanket exception to the warrant requirement, stating that they are only used during "exigent circumstances." By asserting this exception, the policy tacitly acknowledges that use of Situational Awareness Cameras implicates the Fourth Amendment warrant requirement but fails to provide any further information to back up this legal conclusion. This is especially problematic when use of these devices specifically implicates the *Handschu* Consent Decree.

[74] *People v. Rodriguez*, 19 N.Y.3d 166 (2012).

[75] *People v. Bialostok*, 80 N.Y.2d 738, 745 (1993) (internal citations omitted); *see also People v. Darling*, 95 N.Y.2d 530, 535 (2000) ("Because electronic surveillance is singularly invasive, law enforcement officials may intercept communications only when they scrupulously follow constitutional and statutory requirements."); *People v. Rabb*, 16 N.Y.3d 145 (2011) (noting that "[t]he Legislature sought, through its enactment of CPL article 700, to balance competing policies, namely, the protection of '[t]he right of privacy, to which unsupervised eavesdropping poses a great threat . . . against society's interest in protecting itself against crime'") (citing Report of New York State Joint Legislative Committee On Crime, Its Causes, Control & Effect on Society, 1968 NY Legis Doc No. 81, at 44).

[76] *Bialostok*, 80 N.Y.2d at 745 (internal citations omitted).

[77] *Id*. at 744.

To fully comply with the mandates of the POST Act, the policy must fully detail the training officers receive regarding the legal and constitutional implications of use of the devices. That training must include proper guidance on when and how court authorizations may be required, as well as detail which personnel are authorized to evaluate a situation and approve of its use. There must also be an auditing policy to report on how and when Situational Awareness Cameras are employed to assure that their use conforms to constitutional and legal requirements.

P. Thermographic Cameras

The draft Thermographic Cameras Impact and Use Policy states that thermographic cameras must be used in a manner consistent with the Constitution of the United States, the New York State Constitution, and any applicable statutes. However, the policy further insists that "[t]he NYPD does not seek court authorization prior to use of thermographic cameras," and that the devices are only used "during emergencies where exigent circumstances exist or to conduct surveillance of locations exposed to public observation."

In *Kyllo v. United States*,[78] the United States Supreme Court held that the use of a thermographic cameras aimed at a private residence from a public street constituted a search under the Fourth Amendment.[79] The holding in *Kyllo* contradicts the policy's assertion that a warrant is unnecessary to surveil locations exposed to public observation with a thermographic camera. The policy should be redrafted to explain how the NYPD will abide with the Supreme Court's decision in *Kyllo* and secure a warrant when necessary.

Q. Unmanned Aircraft Systems (UAS)

The draft Impact and Use Policy states that NYPD uses unmanned aircraft systems ("UAS") to "conduct search and rescue missions, disaster response, documentation of traffic collision and crime scenes, crowd monitoring and provide a bird's eye view in dangerous active shooter and hostage situations." The policy further states that the "UAS do not use artificial intelligence,

[78] 533 U.S. 27 (2001).

[79] *Id*. at 40 ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without public intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.").

machine learning, video analytics, or facial recognition technologies." The only biometric measuring capability is the processing of thermal data through thermographic cameras. However, although the policy disclaims use of artificial intelligence, video analytics, and facial recognition, it does not explain whether the UAS are *capable* of using these technologies, which is important for the public to be able to fully understand the implications of such technologies especially as their use evolves. Automated UAS are a reality and currently deployed in Chula Vista, California.[80] Automated drones use technology similar to that in self-driving cars to fly to and from a location. Furthermore, even if a drone is not equipped with facial recognition software that scans for faces in real-time, video surveillance acquired by a UAS can be fed into facial recognition program run by the NYPD's Facial Identification Section or a third party like Clearview AI. The policy does not include any restrictions or policy statements related to the use of UAS-acquired video in facial recognition software.

The policy also includes an unclear structure for the deployment of UAS. The policy states:

> NYPD policy directs that UAS may be used for the following purposes: search and rescue operations, documentation of collisions and crime scenes, evidence searches at large inaccessible scenes, hazardous material incidents, monitoring vehicular traffic and pedestrian congestion at large scale events, visual assistance at hostage/barricaded suspect situations, rooftop security observations at shooting or large scale events, public safety, emergency, and other situations with the approval of the Chief of Department.
>
> UAS cannot be used for routine foot patrol by officers; traffic enforcement or immobilizing a vehicle or suspect.

This statement in the policy contradicts itself and fails to inform the public as to when UAS may be used by the NYPD. First, the policy appears to allow UAS deployment to monitor vehicular and pedestrian traffic at "large-scale events" while also banning deployment for traffic enforcement. The policy does not adequately explain how monitoring vehicular and pedestrian traffic at large-scale events is different than traffic enforcement. The term "large-scale event" is not defined in the policy and New York City's status as the largest city in the United States means that many routine events could be considered "large-scale." Second, by permitting UAS deployment for "public safety,

[80] *See* Cade Metz, *Police Drones Are Starting to Think for Themselves*, New York Times, Dec. 5, 2020, available at https://www.nytimes.com/2020/12/05/technology/police-drones.html [last accessed Feb. 11, 2021].

emergency, and other situations with the approval of the Chief of Department," the policy effectively removes any practical limitation on UAS deployment. Furthermore, if the policy delegates the authority to deploy UAS to the Chief of Department, then there should be clear guidelines governing this decision. Additionally, despite many of these restrictions existing under Patrol Guide section 212-124 (Use of Department Unmanned Aircraft System (UAS)), the NYPD has previously used drones over Pride March,[81] the Women's March,[82] and the Puerto Rican Day Parade.[83]

The policy also includes an unclear decision-making chain for UAS deployment. According to the policy, the decision to deploy UAS "must be made by an NYPD executive serving as a commanding officer, executive officer, or daily duty captain." This person makes the request to NYPD's Technical Assistance Response Unit (TARU). TARU personnel "assess whether such use comports with NYPD policy" among other factors. If a disagreement occurs, a TARU supervisor is consulted and, if the disagreement cannot be resolved, the "daily duty chief will make the final determination." However, this decision structure does not include a role for the Chief of Department. The policy appears to simultaneously vest final decision making on UAS deployment in both the Chief of Department and in the daily duty chief. The policy should be revised to clarify this authority and the appropriate decision-making authority.

Finally, regarding the disparate impact of this technology, the policy appears to erroneously reference the safeguards and audit protocols for Body Worn Cameras (BWC). There is no other reference or cite to the BWC Impact and Use Policy in the policy. The policy should be revised to correct this error and explain how the safeguards and audit protocols built into the UAS mitigate the risk of disparate or biased policing.

[81] Unmanned Aircraft System (UAS) Deployment Report (PD 620-151) for June 30, 2019, obtained by the Legal Aid Society via a Freedom of Information Law request, available at https://docdro.id/10qjsk0 [last accessed Feb. 23, 2021].
[82] Mark Chiusano, *Eye in the sky*, Newsday, Sept. 30, 2020, available at https://www.newsday.com/opinion/columnists/mark-chiusano/mark-chiusano-nassau-police-drones-long-island-protests-surveillance-1.49894779 [last accessed Feb. 23, 2021].
[83] Unmanned Aircraft System (UAS) Deployment Report (PD 620-151) for June 9, 2019, obtained by the Legal Aid Society via a Freedom of Information Law request, available at https://docdro.id/sed2rWP [last accessed Feb. 23, 2021].

R. WiFi Geolocation Devices

The WiFi Geolocation Devices draft policy demonstrates the strengths and weaknesses of the POST Act legislation; the policy revealed a surveillance tool that the public was previously unaware the NYPD possessed and at the same time the policy fails to provide sufficient information and safeguards.

Just as cell-site simulators require an eavesdropping warrant, so should the WiFi geolocation device. Based on the draft policy, the NYPD would not even require a warrant but only "a court order" after the device was already used or in use. Considering the NYPD's access to New York City courts and the ease in which both the search warrant and eavesdropping statues allow for emergency applications, it should be rare – if ever – that the NYPD should be allowed to use a WiFi geolocation device without the bare minimum judicial scrutiny of a search warrant application.

Even assuming obtaining a court order after the fact would be a sufficient safeguard, the policy does not even list what type of court order is required or the authority for it to be issued. Notably, unlike the cell-site simulator policy, the WiFi geolocation device policy does not have any requirement that the order be based upon probable cause. The policy initially implies the order must be based upon probable cause – "WiFi geolocation tracking devices may be deployed prior to obtaining a probable cause order" – but the description of the process to obtain an order does not explicitly require a showing of probable cause. As a result, it leaves unclear if it is an acceptable procedure to obtain a court order not based upon probable cause post-use of the WiFi geolocation device. It also does not provide any remedy if a court were to deny an application for such an order, after the device had already been used. Additionally, like the cell-site simulator policy, there is no explanation for the type of order or the authority under which it would be issued. An eavesdropping warrant would be the most appropriate avenue, but the policy in its current form does not even require the less onerous search warrant or even a judicial finding of probable cause.

III. Missing Policies

A. GPS Pinging/Exploitation of the E-911 System

GPS pinging is when a signal is sent by a cellular service provider to a target phone through the Enhanced 911 System (E-911), forcing the phone to send its location to the service provider and exploiting a feature that is intended to be used to find someone who has an emergency and has called 911. The service provider then reports to the police the GPS coordinates. Cell phone service companies are only conducting GPS pinging when a person calls 911 or at the behest of law enforcement. The owner or possessor of the phone is not aware that any of this is occurring and the only way to prevent it would be to shut the phone off. The pinging of the target phone often occurs multiple times an hour for extended periods of time. In *People v. McDuffie,*[84] the NYPD forced the phone company to ping Mr. McDuffie's phone 3,275 times over fourteen days, getting precise GPS coordinates of the location of the phone each time.

Except when there are exigent circumstances, the phone companies require a court order, search warrant, or an eavesdropping warrant before they will perform GPS pinging and provide the results to law enforcement. Like cell-site simulators, the use of GPS pinging should require an eavesdropping warrant, but the NYPD typically only obtains a pen register/trap-and-trace order or at most a search warrant.

In *People v. Hernandez,*[85] Justice Matthew J. D'Emic correctly identified and analyzed the issues involving GPS pinging, finding that the use of GPS pinging required probable cause and "fits into the statutory scheme for eavesdropping and visual surveillance warrants."[86] While the Court in *People v. Gordon* was primarily concerned with cell-site simulators, Justice Murphy also found that CPL Article 705 did not authorize the use of GPS: "It should be noted, however, that article 705 does not authorize the gathering of location information using a cell phone's global positioning

[84] 58 Misc.3d 524 (Sup. Ct., Kings Co. 2017).
[85] 56 Misc.3d 586 (Sup. Ct. Kings Co. 2017).
[86] *Id.* at 589.

system (GPS)…”.[87] The Court, citing the Court of Appeals in *People v. Weaver*,[88] continued by stating “that GPS technology is far more intrusive than pen register and/or trap and trace devices” and “[w]ith the requirement of probable cause, a warrant for GPS tracking devices fits into the statutory scheme for eavesdropping and visual surveillance warrants.”[89]

Potentially more concerning than the NYPD’s willingness to use this invasive surveillance technique with minimal justification is how the NYPD handles the notification of the GPS results to its officers and detectives. Based upon discovery received in multiple cases and the investigation by members of the Legal Aid Society’s Digital Forensics Unit, it appears that the NYPD has a system that automatically emails the results to the relevant NYPD investigators. That may be of minimal concern by itself, but the domain address for the sending email was previously registered using false information. The company name appeared to be for a non-existent company, the phone number used a NYC area code and then just the same digit over and over, and the physical address did not exist. The only piece of legitimate information used for the website/email domain registration was an AOL email address. The AOL email address appeared to be a personal account of a detective known to be a member of the NYPD’s Technical Assistance Response Unit (TARU) and his wife. When the domain was renewed, a separate set of similarly false information was used.

It is troubling that the NYPD is attempting to hide this domain from regulation and oversight, and it is unclear if even the appropriate NYPD personnel are aware of this practice. Additionally, it brings up significant questions about the protection of the highly sensitive data that is coming through and potentially stored by this system and the connected email accounts. Compounding this concern is the fact that the NYPD has not provided a draft policy for its use of the GPS pinging technique nor for the results it generates.

B. Rapid DNA Technology

During a 2017 meeting of the New York State Commission on Forensic Science (“the Commission”), the NYPD’s Chief of Forensics said that the Department had purchased Rapid DNA

[87] 58 Misc.3d 544, 547 (Sup. Ct., Kings Co. 2017).
[88] 12 N.Y.3d 433 (2009).
[89] *Gordon* at 548-549.

machines and intends to use them "enhance [the NYPD's] forensic capabilities portfolio."[90] At the same time, members of the Department have been working with other forensic practitioners on experiments using this technology on crime scene evidence.[91] These machines, which allow police to develop DNA profiles from individuals at the police precinct,[92] is precisely the type of surveillance contemplated by the POST Act. Yet there is no mention of it among the NYPD's draft policies.

The omission of *any* mention of Rapid DNA raises serious concerns about the completeness of the draft policy disclosures. More important, it leaves New Yorkers in the dark about critical issues concerning Rapid DNA, including: (1) the NYPD's use of the technology and what, if any, limitations may be placed on it; (2) the way that data is secured within this technology; and (3) the measures, if any, to ensure that this technology is used reliably and responsibly.

Rapid DNA is a surveillance tool. It allows NYPD officers to collect DNA from individuals while they are detained at the police precinct and, within 90 minutes, develop their full forensic profiles, entirely within the confines of the stationhouse.[93] These DNA samples may be taken through buccal swabs, or, as in more than half of the instances of DNA collection,[94] surreptitiously through bringing a person into an interrogation room to secretly collect their DNA.[95] Once taken, DNA profiles from individuals may be housed within the internal NYPD DNA index – which has been widely criticized for lacking a legal foundation and circumventing state regulations governing

[90] Kevin Deutsch, *Exclusive: NYPD Plans to Use Controversial "Rapid DNA" Technology as Early as 2019*, Feb. 22, 2019, available at https://bronxjusticenews.com/exclusive-nypd-plans-to-use-controversial-rapid-dna-technology-as-early-as-2019/ [last accessed Feb. 23, 2021].
[91] A.A. Mapes, et al., *Decision support for using mobile Rapid DNA analysis at the crime scene*, Sci Justice, Jan. 2019, available at https://pubmed.ncbi.nlm.nih.gov/30654966/ [last accessed Feb. 23, 2021].
[92] Heather Murphy, *Coming Soon to a Police Station Near You: The DNA Magic Box*, New York Times, Jan. 21, 2019, available at https://www.nytimes.com/2019/01/21/science/dna-crime-gene-technology.html [last accessed Feb. 23, 2021].
[93] *Id.*; *see also* ThermoFischer Scientific, *Rapid DNA Solutions—Because Every Minute Counts*, available at https://www.thermofisher.com/us/en/home/industrial/forensics/human-identification/forensic-dna-analysis/dna-analysis/rapidhit-id-system-human-identification.html [last accessed Feb. 23, 2021].
[94] Erin Durkin, *Cops take heat from Council over DNA, despite promised reforms*, Politico, Feb. 25, 2020, available at https://www.politico.com/states/new-york/albany/story/2020/02/25/cops-take-heat-from-council-over-dna-despite-planned-reforms-1263552 [last accessed Feb. 23, 2021].
[95] George Joseph, *How Juveniles Get Caught Up in the NYPD's Vast DNA Dragnet*, Gothamist, Jan. 10, 2019, available at https://gothamist.com/news/how-juveniles-get-caught-up-in-the-nypds-vast-dna-dragnet [last accessed Feb. 23, 2021].

DNA indexing – or it may be shared with private, for-profit companies like Smallpond.[96] These uses violate the New York State Executive Law,[97] which requires that all forensic testing be validated and approved by the State Commission on Forensic Science, bars private municipal DNA indexing, and prohibits warrantless DNA collection from people who are not convicted of crime.[98] Indeed, there is nothing within New York State or City law that permits the NYPD to use Rapid DNA. Yet while the Department purchased this technology, and announced its intention to use it, it has provided no public information about what, if any, limitations may be placed on it. This lack of candor is troubling from a Department that conducted race-based DNA dragnets,[99] stole DNA from children as young as 12,[100] and has filled the City-run DNA rogue index with almost 34,000 people.[101]

In addition to not providing any limitations on its use, the NYPD has refused to disclose what, if any, measures are taken to secure genetic information stored in City, private, or other unregulated databases. As noted above, the NYPD's fingerprint database already was infected by malware. A trove of New Yorkers' DNA would be an even more attractive target for hackers, with even more devastating consequences. Indeed, media reports widely document China's keen interest in growing DNA databases,[102] including by contracting with the same companies with which the NYPD may be working at this very moment.[103] There also is no way of knowing whether the NYPD will share their data with immigration officials. This also is an imminent threat, given those agencies' aggressive goals in collecting and indexing DNA.

[96] *See* Smallpond: DNA Matching System, available at https://www.smallpondllc.com/ [last accessed Feb. 23, 2021].

[97] *See* N.Y. Exec. L. 995-b (requiring Commission review of DNA technologies).

[98] *See People v. Goldman*, 35 N.Y.3d 582, 585 (2020) (warrant required for corporeal evidence, including DNA).

[99] Jan Ransom & Ashley Southall, *'Race-Biased Dragnet': DNA From 360 Black Men Was Collected to Solve Vetrano Murder, Defense Lawyers Say*, New York Times, Mar. 31, 2019, available at https://www.nytimes.com/2019/03/31/nyregion/karina-vetrano-trial.html [last accessed Feb. 23, 2021].

[100] Jan Ransom & Ashley Southall, *N.Y.P.D. Detective Gave a Boy, 12, a Soda. He Landed in a DNA Database,* New York Times, Aug. 15, 2019, https://www.nytimes.com/2019/08/15/nyregion/nypd-dna-database.html [last accessed Feb. 23, 2021].

[101] *See* NYC OCME Local DNA Index System (LDIS) Statistics, Feb. 1, 2021, available at https://www1.nyc.gov/assets/ocme/downloads/pdf/ldis020121.pdf [last accessed Feb. 23, 2021].

[102] David Cyranoski, *China's massive effort to collect its people's DNA concerns scientists,* Nature, July 7, 2020, available at https://www.nature.com/articles/d41586-020-01984-4 [last accessed Feb. 23, 2021].

[103] Sui-Lee Wee, *China is Collecting DNA from Tens of Millions of Men and Boys, Using U.S. Equipment*, New York Times, Jun. 17, 2020, available at https://www.nytimes.com/2020/06/17/world/asia/China-DNA-surveillance.html [last accessed Feb. 23, 2021].

Finally, by omitting any mention of Rapid DNA in the draft policy, the NYPD provides no assurance that this surveillance technology is or will be used in a reliable manner. Unlike the Office of the Chief Medical Examiner, which provided public reports to the Commission its laboratory-based use of Rapid DNA,[104] the NYPD has never publicly disclosed how it uses this technology. This is critical: the FBI,[105] the National District Attorney's Association,[106] and the National Institute of Science and Technology[107] all advocate for a limited use of Rapid DNA, and only after an extended and searching validation process. Without this, we are kept in the dark about not just how people's DNA is being tracked and surveilled by the NYPD but also whether it is even being done in a scientifically responsible and reliable manner.

IV. Conclusion

The draft policies released on January 11, 2021 do not satisfy the requirements or purpose of the POST Act. The NYPD needs to overhaul its approach to these policies, focusing on true transparency. If the finalized policies continue to fail to meet the objectives of the POST Act, the City Council's Committee on Public Safety should hold a hearing on the NYPD's unwillingness or inability to comply.

Sincerely,
The Legal Aid Society of New York City

Cc: NYC Mayor Bill de Blasio (Via Email & U.S. Mail)
NYC Council Speaker Corey Johnson (Via Email & U.S. Mail)
NYC Council Public Safety Committee Chair Adrienne E. Adams (Via Email & U.S. Mail)
NYC Council Member Vanessa L. Gibson (Via Email & U.S. Mail)

[104] New York State DNA Subcommittee Draft Meeting Minutes, May 17, 2019, available at https://www.criminaljustice.ny.gov/pio/open-meetings/5-17-2019-dna/Meeting-Minutes.pdf [last accessed Feb. 23, 2021].

[105] FBI, *Rapid DNA*, available at https://www.fbi.gov/services/laboratory/biometric-analysis/codis/rapid-dna [last accessed Feb. 23, 2021].

[106] National District Attorneys Association, *NDAA Position Statement on Use of Rapid DNA Technology*, Jan. 30, 2018, available at https://dps.alaska.gov/getmedia/fb933229-8e52-4cf8-8fe0-cb72d5e039e3/NDAA-Statement-on-Use-of-Rapid-DNA-Technology-2018.pdf [last accessed Feb. 23, 2021].

[107] Eric Romsos & Peter Vallone, *2018 Rapid DNA Maturity Assessment*, Applied Genetic Group, NIST, Nov. 7, 2018, available at https://www.nist.gov/system/files/documents/2018/11/14/3_romsos.pdf [last accessed Feb. 23, 2021].