Committee on Public Safety
Deepa Ambekar, Committee Counsel
Beth Golub, Legislative Counsel
Casie Addison, Legislative Policy Analyst
Steve Riester, Senior Financial Analyst

THE COUNCIL OF THE CITY OF NEW YORK

Committee Report of the Governmental Affairs Division
Matthew Gewolb, Legislative Director
Rachel Cordero, Deputy Director, Governmental Affairs Division

COMMITTEE ON PUBLIC SAFETY
Hon. Vanessa Gibson, Chair

June 14, 2017

INT. NO. 1482:	By Council Members Garodnick, Gibson, Lander, Vacca, Gentile, Koslowitz, Kallos, Dromm, Rodriguez, Rosenthal, Mendez, Levine, Johnson, Perkins and Menchaca
TITLE:	A Local Law to amend the administrative code of the city of New York, in relation to creating comprehensive reporting and oversight of NYPD surveillance technologies.
ADMINISTRATIVE CODE:	Adds a new section 14-167.

I. INTRODUCTION

On June 14, 2017 the Committee on Public Safety, chaired by Council Member Vanessa Gibson, will hear Introductory Bill Number 1482 (Int. 1482), a local law to amend the administrative code of the city of New York, in relation to creating comprehensive reporting and oversight of NYPD surveillance technologies. Among those expected to testify include representatives from the New York City Police Department (NYPD or Department), advocates, and members of the public.

II. BACKGROUND

Over the last several years, there has been growing concern and attention regarding law enforcement's acquisition and use of new and invasive surveillance technologies.[1] These technologies include devices such as military grade X-Ray vans, license plate readers and cell site simulators that can capture cell phone information from surrounding cell phone users.[2] At the local level, there is little to no public comment, governmental oversight or legislative input in the acquisition and use of these technologies. Often, law enforcement's use of such technologies is only revealed through litigation. Privacy rights advocates believe there is a need for greater police transparency regarding the use of surveillance technology.[3]

Although advocates seek greater transparency regarding NYPD's use of surveillance technologies, the Department believes that the reporting of this information would empower terrorists and criminals by revealing all of the available law enforcement tools.[4] The NYPD

---

[1] "New Bill Holds NYPD Accountable for Surveillance Technology" available at https://www.aclu.org/news/new-bill-holds-nypd-accountable-surveillance-technology

[2] Id.

[3] https://www.aclu.org/news/new-bill-holds-nypd-accountable-surveillance-technology

[4] "NYPD Blasts Surveillance Transparency Bill as Boon to 'Terrorist'" available at https://www.dnainfo.com/new-york/20170302/civic-center/post-bill-nypd-spy-technology

maintains that disclosing the types of surveillance equipment being used will allow illicit actors to develop counter technologies to evade detection.[5]

III. NYPD USE AND DISCLOSURE OF SURVEILLANCE TECHNOLOGIES

a. Cell Site Simulators

In February of 2016, the NYPD confirmed, in response to a Freedom of Information Law (FOIL)[6] request, that it owns and uses Stingrays, a type of cell-site simulator that can be used to track the location, identifying information, and content of nearby cell phones.[7] Specifically these cell-site simulators are devices that mimic a cell tower, and allow the police to pinpoint a person's location and, in some configurations, collect the phone numbers that a person has been texting and calling and intercept the contents of communications.[8] Additionally, if these devices are used at a mass gathering, they can collect cell phone information from a nearby bystanders' cell phone.[9]

According to the FOIL disclosure, the NYPD stated that it used Stingrays 1,016 times between 2008 and May 2015 without a written policy for when and how to do so, except in some situations the Department obtains a "pen register order."[10] A pen register order is a court order, which is granted on "reasonable suspicion" that a crime has, or is being committed, and the use of a pen register is or will be relevant to an "ongoing criminal investigation."[11] A pen register order has a lower legal standard of "reasonable suspicion" than the more stringent "probable cause" requirement for a court to issue a search warrant.[12] In July of 2016, however, the Southern District

---

[5] Id.
[6] Public Officers Law §87 et.seq.
[7] "NYPD Has Used Stingrays More Than 1,000 Times Since 2008" *available at* https://www.nyclu.org/en/press-releases/nypd-has-used-stingrays-more-1000-times-2008
[8] Id.
[9] Id.
[10] Id.
[11] C.P.L. §705.10
[12] Id. at §690 et. al.

of New York held that the use of a cell-site simulator constituted a search under the Fourth Amendment and therefore required law enforcement to apply for a search warrant.[13]

b. BackScatter Van

In addition to cell site simulators, the NYPD has reportedly used X-ray vans, or "Z BackScatter Vans." These are military-grade vans that enable officers to "look through" walls of buildings or sides of trucks using X-ray radiation.[14] Each of these vans cost an estimated $729,000 to $825,000.[15] Though the NYPD has not disclosed when, where or how often this technology is used, former Police Commissioner Bill Bratton stated that the equipment was not used to scan people for weapons.[16]

In an effort to find additional information, the news organization ProPublica filed a FOIL request seeking disclosure of the Department's use of Z Backscatter Vans.[17] Generally, the FOIL request sought: 1. a list of past deployments of the Z Backscatter Van; 2. department policies, procedures, and training material for the technology; 3. any legal opinion regarding what situations the surveillance technology could be used; 4. any contracts regarding the purchase of the equipment; 5. any tests or reports regarding health and safety concerns of the van; 6. any records related to data storage and privacy protections; and 7. the contents of image databases used or created by the equipment.[18] The NYPD denied the request to disclose the information on the grounds that the disclosure of the information would "reveal criminal investigation techniques and procedures."[19] ProPublica then filed an Article 78 proceeding to compel the Department to comply

---

[13] *U.S. v. Lambis*, 197 F. Supp. 3D 606 (SDNY 2016)
[14] "The NYPD Is Using Mobile X-Ray Vans to Spy on Unknown Targets," *available at* https://www.theatlantic.com/politics/archive/2015/10/the-nypd-is-using-mobile-x-rays-to-spy-on-unknown-targets/411181/
[15] Id.
[16] Id.
[17] Verified Petition at 7, Grabell v. NYPD, Index No. 13100580 (Sup. Ct. NY 2013)
[18] Id.
[19] Id.

with the FOIL law. The lower court granted the request and required the NYPD to turn over records related to when and where the vans had been used, its policies on van usage and how much they cost.[20] The Department appealed the decision and the First Department overturned the lower court's ruling. The highest court agreed that NYPD's concerns of terrorism outweighed public interest and required that the NYPD only disclose the public health risks associated with the use of the vans.[21]

c. Domain Awareness System

NYPD's Domain Awareness System ("DAS") was developed in partnership with Microsoft and funded through a combination of City funding and a federal Homeland Security Grant.[22] The customized software ties information from city surveillance cameras, license plate readers, and radiation and gunshot detectors to 911 calls, criminal records and other city databases.[23] All the information is accessible and displayed on a "user-friendly" database.

The Department operates about 500 license plate readers throughout the City and saves the collected license plate data for at least five years regardless of whether a car triggers any suspicion.[24] These readers can be mounted on police cars, fixed on poles or roadside to scan the license plates of all cars passing by and capture, at minimum, the license plate number as well as the date, time, and location the car is observed.[25] The plates are quickly compared to "plates of interest."[26] These "plates of interest" are included on a "hot list" that is downloaded into a license

---

[20] In re Grabell v. NYPD, 47 Misc. 3d 203 (Sup. Ct. NY 2014)
[21] In re Grabell v. NYPD, 139 A.D. 3d 477 (1st Dep't 2016)
[22] "NYPD expands surveillance net to fight crime as well as terrorism" available at https://www.aclu.org/blog/free-future/documents-uncover-nypds-vast-license-plate-reader-database http://www.reuters.com/article/usa-ny-surveillance-idUSL2N0EV0D220130621
[23] Id.
[24] "Documents Uncover NYPD's Vast License Plate Reader Database" available at https://www.aclu.org/blog/free-future/documents-uncover-nypds-vast-license-plate-reader-database
[25] "Automatic License Plate Readers" available at https://www.nyclu.org/en/automatic-license-plate-readers
[26] Suggested Gidelines: Operation of License Plate Readers Technology 2011 available at http://www.criminaljustice.ny.gov/ofpa/pdfdocs/finallprguidelines01272011a.pdf

plate reader, and may include data from individuals on the terrorist watch list or stolen cars.[27] If a license plate of a passing car matches a "plate of interest," the system sends an alert.[28] Advocates believe that these license plate readers raise privacy concerns because every license plate is scanned regardless of whether the plate is on the "hot list."[29] These readers could collect information of vehicles parked at addiction counseling meetings, doctor's offices, or even staging areas for political protests.[30] Early last year, the Department was planning to enter into a multi-year contract of more than $400,000, which would give it access to the nationwide database of license plate reader data, owned by the company Vigilant Solutions. The contract would expand the Department's capabilities by providing access to real-time and historical license plate records from around the country.[31] The Vigilant Solutions contract would also greatly expand the NYPD's capabilities by accessing a database that is populated by privately operated license plate readers.[32] Unlike law enforcement scanners that are generally mounted at major intersections, private scanners can be mounted in apartment complexes, malls, or residential streets.[33] This access to the records from around the country could give the NYPD the ability to monitor a vehicle's movement from, for example Staten Island to Seattle.[34] The Vigilant Solutions software also has a "stakeout" option that would allow law enforcement officers to track which cars are commonly seen at a given location or likely locations for a given car.[35] Though the software has these capabilities, the NYPD guidelines for DAS prohibit this sort of use.[36] Civil rights advocates

---

[27] "Automatic License Plate Readers" available at https://www.nyclu.org/en/automatic-license-plate-readers
[28] Id.
[29] Id.
[30] Id.
[31] "The NYPD Is Tracking Drivers Across the Country Using License Plate Readers" available at http://gothamist.com/2016/01/26/license_plate_readers_nypd.php
[32] Id.
[33] Id.
[34] Id.
[35] Id.
[36] Id.

maintain this ability to monitor an individual's location infringes on personal privacy and is akin to the government placing a GPS device on a person's car, thus requiring greater protection and oversight on the law enforcement's usage of the technology as held by the Supreme Court in *Grady v. North Carolina*.[37]

IV. LAWS IN OTHER JURISIDICTIONS

In recent years, some other jurisdictions have passed local laws regulating and requiring reporting on local law enforcement's use of surveillance equipment. In 2013, Seattle and Spokane, Washington, passed legislation that require city council approval prior to acquiring new surveillance equipment by law enforcement.[38] In Oakland, California, the city council created a privacy and data retention advisory committee. In addition to the creation of the advisory committee, the city established a "Citywide Surveillance Technology Ordinance" to create a consistent public process for the council to evaluate surveillance technologies before law enforcement acquires them.[39] In 2016, the state of California passed two laws that require agencies to draft and publicly post privacy and usage policies if their law enforcement uses automated license-plate recognition software or cell site simulators.[40]

V. FEDERAL REPORTING REQUIREMENTS OF SURVEILLANCE EQUIPMENT

There are several federal laws governing public disclosure of information. The Privacy Act of 1974, governs federal collection, use, and disclosure of personally identifiable information

---

[37] Id. *See Also* Grady v. North Carolina, 575 U.S. ___ (2015).
[38] Seattle, Wash., Ordinance 124142 (Mar. 27, 2013), *available at* http://clerk.seattle.gov/~archives/Ordinances/Ord_124142.pdf; see generally SPOKANE, WASH., MUNICIPAL CODE ch. 01.08, (2013), available at https://my.spokanecity.org/smc/?Chapter=01.08
[39] Ali Winston, Oakland Cops Quietly Acquired Social Media Surveillance Tool, EAST BAY EXPRESS (Apr. 13, 2016), http://www.eastbayexpress.com/oakland/oakland-cops-quietly-acquired-social-media-surveillance-tool/Content?oid=4747526.
[40] Cal. Gov. Code §531266 and Cal. Civ. Code §1798.90.5 et. al.

that is maintained in systems of records by federal agencies.[41] Disclosure is required for records under the control of a federal agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.[42] The agencies are required to give public notice of their systems of records by publication in the Federal Register. In addition, the Act prohibits the disclosure of a record about an individual from a system of record absent written consent of the individual unless the disclosure is pursuant to one of the statutory exceptions.[43]

The E-Government Act of 2002 requires all federal government agencies that develop or obtain new technology involving the collection, maintenance, or dissemination of personal information in an identifiable form to publish a Privacy Impact Assessment (PIA).[44] The purpose of the PIA is to demonstrate that the system owners and developers have incorporated privacy protections throughout the entire life cycle of a system. These documents are to be performed and updated as necessary as system changes create new privacy risks.[45] The PIAs are publically available unless the disclosure of the document would raise security concerns or reveal classified information. While law enforcement and national security databases are exempt from some of these transparency requirements, the Federal Bureau of Investigation[46] and Department of Homeland Security[47] regularly publish privacy impact assessments.

In addition, the Administrative Procedure Act (APA) requires federal agencies to engage in public rulemaking under certain circumstances relating to the use of surveillance technology.[48]

---

[41] Privacy Act of 1974, Pub. L. No. 93-5795 § 2(A)(4), 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (2012)
[42] Id.
[43] https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition
[44] Public Law 107-347, 44 U.S.C. §101
[45] M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 *available at* https://www.whitehouse.gov/omb/memoranda_m03-22
[46] https://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system
[47] https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_elsur.pdf
[48] See 5 U.S.C. § 553 (2012)

For example, the Transportation Security Administration was required to conduct rulemaking regarding its use and adoption of "Advanced Imagining Technology" or the "naked scanners[49]"

More recently, the Department of Justice (DOJ) published guidance on its use of cell site simulator technologies, which disclosed information on how this equipment works, how DOJ uses them, how data is collected and retained, and called for agency components to obtain a warrant prior to the use of such technology.[50] In addition, it established training protocols on privacy and civil liberties. Similarly, the DOJ has issued guidelines for agency use of "unmanned aircraft systems," or drones.[51]

VI. ISSUES AND CONCERNS

The Committee is interested in learning about the balance between proper oversight and transparency over NYPD's use of surveillance equipment without compromising public safety. While we appreciate the issues surrounding public safety, we would like to understand what information the Department can disclose without compromising our safety. Specifically, we want to learn more about particular data retention and privacy protection policies the Department has for these technologies. In addition, we want to discuss the Department's legal authority to use certain types of equipment, and who in the department is trained and authorized to use various technologies.

VII. ANALYSIS OF INT. NO. 1482

Section 1 of Int. No. 1482 adds a new administrative code section 14-167 that creates comprehensive reporting and oversight of NYPD surveillance technologies. The first

---

[49] See Electronic Privacy Information v. Department of Homeland Security, 653 F.3d 1 (D.C. Cir. 2011)

[50] DEPARTMENT OF JUSTICE, POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY (undated), available at https://www.justice.gov/opa/file/767321/download.

[51] DEPARTMENT OF JUSTICE, POLICY GUIDANCE: DOMESTIC USE OF UNMANNED AIRCRAFT SYSTEMS (UAS) (undated), *available at* https://www.justice.gov/file/441266/download

subdivision defines "surveillance technology" and the "surveillance technology impact and use policy" (IUP). The IUP is a document that requires the NYPD to report on the: a. capabilities of the surveillance technology; b. rules processes and guidelines regulating access to it, including whether the department obtains a court authorization for each use of the equipment; c. security measures to protect the information collected by the technology; d. policies and practices related to the data retention; e. policies and practices related to access or use of data by members of the public; f. whether other entities outside the Department have access to the data collected by the surveillance technology; g. whether training is required prior to use of the surveillance technology; h. a description of internal audit or oversight mechanisms to comply with the IUP; and i. any tests or reports regarding the health and safety effects of the surveillance technology. The bill requires the Department to propose an IUP and post it on the website prior to the use of new surveillance technology. For existing technology, the NYPD shall propose an IUP within 180 days of the effective date of the bill. When the Department seeks to acquire or acquires enhancements to the surveillance technology that has not previously been disclosed in an IUP, the NYPD must publish an addendum to the existing IUP. Upon the publication of any proposed IUP, the public shall have 45 days to submit comments to the NYPD Police Commissioner. The Police Commissioner shall consider the public comments and provide the final IUP to the council and the mayor, and post it to the Department's website within 45 days after the close of the public comment period.

Section 2 of the bill requires the Inspector General for the Police Department (NYPD-IG) to prepare an annual audit to assess NYPD's compliance with the terms of the IUP. In addition, the NYPD-IG should describe any known or reasonably suspected violations of the IUP and publish recommendations.

Section 3 of Int. 1482 would have the bill take effect immediately.

Int. No. 1482

By Council Members Garodnick, Gibson, Lander, Vacca, Gentile, Koslowitz, Kallos, Dromm, Rodriguez, Rosenthal, Mendez, Levine, Johnson, Perkins and Menchaca

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

Be it enacted by the Council as follows:

Section 1. Chapter 1 of title 14 of the administrative code of the city of New York is amended by adding a new section 14-167 to read as follows:

§ 14-167. Annual surveillance reporting and evaluation.

a. Definitions. As used in this section, the following terms have the following meanings:

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

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

2. parking ticket devices;

3. technology used primarily for internal department communication; or

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

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

1. a description and capabilities of a surveillance technology;

2. rules, processes and guidelines issued by the department regulating access to or use of such surveillance technology as well as any prohibitions or restrictions on use, including whether

the department obtains a court authorization for each use of a surveillance technology, and what specific type of court authorization is sought;

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

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

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

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

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

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

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

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

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

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

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

f. The commissioner shall consider public comments and provide the final surveillance technology impact and use policy to the council and the mayor, and shall post it to the department's website at most 45 days after the close of the public comment period, pursuant to subdivision d of this section.

§ 2. Chapter 34 of the New York city charter is amended by adding a new section 809 to read as follows:

§ 809. Surveillance technology impact and use policy. a. For the purposes of this section, the following terms have the following meanings:

"Inspector general for the police department" means the individual responsible for implementing the duties set forth in paragraph 1 of subdivision c of section 803 of this chapter.

b. The inspector general for the police department shall prepare annual audits of surveillance technology impact and use policies as defined in section 14-167 of the administrative code that shall:

1. assess whether the New York city police department's use of surveillance technology, as defined in section 14-167 of the administrative code, complies with the terms of the surveillance technology impact and use policy;

2. describe any known or reasonably suspected violations of the surveillance technology impact and use policy, including but not limited to complaints alleging such violations made by individuals pursuant section 803(c)(6) of this chapter; and

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

§ 3. This local law takes effect immediately.

LS 6645
DA
1/25/2017