TESTIMONY

The Council of the City of New York
Committee on Public Safety

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

Proposed Int. No. 1482-2017 (Public Oversight of Surveillance Technology (POST) Act)

The Legal Aid Society
Criminal Defense Practice
49 Thomas Street
New York, NY 10013
By: Jerome D. Greco
(212) 298-3075
JGreco@legal-aid.org

June 14, 2017

Good morning. I am Jerome Greco, a staff attorney in the Legal Aid Society's Digital Forensics Unit in the Criminal Practice, a specialized unit providing support for digital evidence and electronic surveillance issues for the Legal Aid Society's attorneys and investigators, in all five boroughs. We thank this Committee for the opportunity to provide testimony on Proposed Int. No. 1482-2017.

ORGANIZATIONAL INFORMATION

Since 1876, The Legal Aid Society has provided free legal services to New York City residents who are unable to afford private counsel. Annually, through our criminal, civil and juvenile offices in all five boroughs, our staff handles about 300,000 cases for low-income families and individuals. By contract with the City, the Society serves as the primary defender of indigent people prosecuted in the State court system. In 2013, the Legal Aid Society created the Digital Forensics Unit to serve and support Legal Aid attorneys and investigators in our criminal defense offices. Consisting of four analysts and one full time staff attorney, members of the Unit are trained in various forms of digital forensics and have encountered multiple different types of electronic surveillance used by law enforcement.

SUPPORT FOR INT. NO. 1482-2017 (POST Act)

We support the proposed amendments to the Administrative Code of the City of New York and the New York City Charter that would require oversight of the purchase and use of surveillance technologies by the New York City Police Department ("NYPD"). The Legal Aid Society's extensive criminal defense practice and digital forensic abilities puts us in a unique position to understand the urgent necessity of Int. No. 1482-2017. Requiring the promulgation of publicly reviewed impact and use policies and oversight of compliance with the policies by the NYPD Inspector General will help ensure that the NYPD's procurement and use of surveillance

technology is not abused and complies with constitutional and statutory restrictions, while not undermining security.

The NYPD appears to be using its increasingly powerful surveillance technologies with few rules, procedures, or guidelines regulating how and when they are used, or what authority is required. Additionally, the methods to store, protect, and/or purge the data collected remain mostly a secret. Secrecy lends itself to misuse and increases the potential for routine and undetected constitutional violations. As will be explained further, the courts, the traditional check on law enforcement abuse or overreach, are not equipped to probe the NYPD's use of surveillance technologies and have been misled about the nature of these technologies. Likewise, defense attorneys have been unable to zealously advocate on behalf of their clients because information about the surveillance technologies often used against them have not been disclosed in the courtroom.

While we are aware of several forms of NYPD surveillance, we will restrict this testimony to cell-site simulators, ShotSpotter, facial recognition, and automated license plate readers. Beyond these, we suspect the NYPD may also have surveillance technologies and methods we currently do not know are in use or in its possession.

A. Cell-Site Simulators ("Stingray" Devices)

Cell-site simulators or IMSI[1] catchers, commonly referred to as Stingrays after a model produced by the Harris Corporation, are devices designed for the military and now marketed to law enforcement that pretend to be cell phone towers in order to force connections from all cell phones in range of the device. Data collected by the cell-site simulator can be used to track an individual, including the capability to locate someone in his or her home by using the signal to

[1] IMSI stands for International Mobile Subscriber Information, an identifying number unique to each phone.

penetrate the walls of the home. Additionally, in an event like a protest or a large concert, it can log the IMSI of every cell phone forced to connect to it for potential use in future investigations.

While we know that the NYPD possesses cell-site simulator devices, we do not know the model or the capabilities of their equipment. Some models have the capability to intercept and record the contents of communications, including phone calls and text messages.[2] This feature appears to be available via software settings and updates. They can also collect information about numbers dialed, duration of calls, and status of calls.[3, 4] Other models even have the capability of installing malware on the user's phone without the user's knowledge.[5]

Beyond being a powerful surveillance tool, cell-site simulators have the capability to interfere with cell phone users' ability to access emergency services and their cell service. 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' phone.[6] Although 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.[7] In other words, if you have the misfortune of being near a cell-site simulator at the time of an emergency, you may not be able to call a loved one and your attempts to call 911 may be thwarted.

---

[2] Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology (indicating the capability of a cell-site simulator to collect contents of communications, "cell-site simulators used by the Department must be configured as pen registers, and may not be used to collect the contents of any communication…") (https://www.justice.gov/opa/file/767321/download)

[3] Electronic Frontier Foundation's "Cell-site simulators: Frequently Asked Questions" (https://www.eff.org/sls/tech/cell-site-simulators/faq)

[4] Documents obtained by the American Civil Liberties Union of Northern California pursuant to a Freedom of Information request (https://www.aclunc.org/docs/20151027-crm_lye.pdf)

[5] "Illinois Sets New Limits On Cell-Site Simulators" (https://www.engadget.com/2016/08/25/illinois-sets-new-limits-on-cell-site-simulators/)

[6] "Feds Admit Stingrays Can Disrupt Cell Service of Bystanders" (https://www.wired.com/2015/03/feds-admit-stingrays-can-disrupt-cell-service-bystanders/)

[7] "RCMP reveals use of secretive cellphone surveillance technology for the first time" (http://www.cbc.ca/news/technology/rcmp-surveillance-imsi-catcher-mdi-stingray-cellphone-1.4056750)

To the extent we know anything about the NYPD's use of cell-site simulators, it is because of freedom of information requests by multiple civil rights groups and media outlets. The NYPD is not the only police department who has been secretive about its use of cell-site simulators. In order to purchase stingray devices, the U.S. Department of Justice required local law enforcement agencies to sign non-disclosure agreements ("NDA").[8] Some of these agreements went as far as requiring criminal cases be dismissed in lieu of disclosing anything about the device.[9, 10] The NYPD signed a similar NDA which requires, even when ordered by a court to reveal the information, to "use its best efforts to make such disclosure in a manner that provides maximum protection of the information to be disclosed."[11]

Thanks to the Freedom of Information Law ("FOIL") litigation by the New York Civil Liberties Union ("NYCLU") we now know the NYPD used a cell-site simulator more than 1,000 times from 2008 through 2015 without any written policy on its use.[12] Despite the NYPD's insistence that many of its surveillance technologies that would be covered by the proposed bill are necessary to prevent terrorism, almost all of the investigations in which a cell-site simulator was used were unconnected to terrorism investigations. The alleged crimes being investigated ranged from homicides to drug crimes and grand larceny.

Even more troubling is that none of the NYPD detectives or District Attorneys involved in those investigations obtained a warrant. As of today, The Legal Aid Society has definitively identified only one open case in which a cell-site simulator was used. Upon the filing of a

---

[8] "Stingray spying: FBI's secret deal with police hides phone dragnet from courts" (https://www.theguardian.com/us-news/2015/apr/10/stingray-spying-fbi-phone-dragnet-police)
[9] "Baltimore Police used secret technology to track cellphones in thousands of cases" (http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html)
[10] Baltimore Police Stingray Non-disclosure Agreement (https://assets.documentcloud.org/documents/1808819/baltimore-police-stingray-non-disclosure-agreement.pdf)
[11] Redacted NYPD and Harris Corporation NDA obtained by the New York Civil Liberties Union pursuant to a FOIL request (https://www.nyclu.org/sites/default/files/Nondisclosure_Agreement_web.pdf)
[12] "NYPD has Used Stingrays More Than 1,000 Times Since 2008" (https://www.nyclu.org/en/press-releases/nypd-has-used-stingrays-more-1000-times-2008)

discovery demand and motion identifying our suspicion that such a device was used, the assigned assistant district attorney buried its concession of a cell-site simulator operation in nine pages of otherwise irrelevant information. We have also identified two other open cases and one closed case, in which a cell-site simulator was likely used, but have not yet been able to confirm our suspicion despite motions being filed in the open cases. While we have the list of the more than 1,000 times that the NYPD used a stingray, identifying closed cases where cell-site simulators were involved remains difficult because of the NYPD's redactions.

The NYPD has made it more difficult for us to identify when cell-site simulators have been used by seeking pen register orders from the court pursuant to C.P.L. §705, instead of warrants under C.P.L. §700. Put simply, the NYPD is misleading the courts. A cell-site simulator is not a pen register and works much differently than a pen register or a trap and trace device. As explained earlier, the simulator is capable of much more than identifying and recording outgoing numbers dialed and origination of numbers of incoming calls, which are the sole capabilities of pen registers and trap and trace devices. Unlike the federal pen register statute, the New York statute was never expanded to include anything that acts even remotely like a cell-site simulator. Moreover, an order for a pen register requires only reasonable suspicion and not a warrant pursuant to probable cause. It also has less conditions and requirements before it can be obtained.[13] A New York Federal Court has, however, already decided that the use of a cell-site simulator requires a warrant under the Fourth Amendment of the U.S. Constitution[14], and logically, its corollary under the New York State Constitution.

Based on our investigation of the previously mentioned Legal Aid Society cases, we now possess more than one pen register order and application we believe to be related to the use of cell-site simulators. At no point do the applications or orders indicate to the presiding judge that

[13] C.P.L. §705.10(2) compared with §700.15(2-5)
[14] United States v. Lambis, 197 F. Supp. 3d 606 (S.D.N.Y. 2016)

the pen register order authorized the use of cell-site simulators. The majority of the details and information provided attempts to mislead the judges to believe that the information is coming from the cellular service providers and is therefore constitutional under the more relaxed standards of the third party doctrine. Besides obscuring the use of the cell-site simulator, how it works, and the effect it has on non-target phones, the reliance on the third party doctrine is misplaced. When cell phone users are involuntarily forced to connect to a cell-site simulator, instead of a commercial cell phone tower, they are not knowingly disclosing their information. Also, the NYPD, obviously a government law enforcement agency, is not a third party.[15]

The deceptive use of pen register orders has impaired the traditional oversight roles of judges in the criminal justice system. The mostly successful attempts to keep the cell-site simulator information from defense counsels has violated their clients' constitutional rights to be free from unwarranted search and seizure and to have effective assistance of counsel. Passing Int. No. 1482-2017 would protect New Yorkers from these ongoing violations.

B. ShotSpotter Detection System

ShotSpotter is an audio surveillance system from SST, Inc. (formerly ShotSpotter, Inc.) that uses triangulation from sensors on public streets to detect gunshot-like sounds and locate what it assumes are gunshots. The NYPD's system currently covers 60 miles of New York City.[16]

The CEO of SST, Ralph A. Clark, has previously claimed that although ShotSpotter detected and recorded audio, it did not record conversations between people.[17] Even at this time, the company claims "human voices do not trigger ShotSpotter sensors."[18] But the company fails

---

[15] Lambis at 614-615.
[16] "Gunfire tracking ShotSpotter will cover more of North Shore" (http://www.silive.com/news/2017/04/gunfire_tracking_shotspotter_w.html)
[17] "Here's How the NYPD's Expanding ShotSpotter System Works" (https://www.dnainfo.com/new-york/20160518/crown-heights/heres-how-nypds-expanding-shotspotter-system-hears-gunfire)
[18] "Privacy Policy" (http://www.shotspotter.com/privacy-policy)

to clarify that the sensors are recording at all times including human voices even if these recordings do not trigger an alert to the police. ShotSpotter is not only capable of recording conversations between people but it also preserves those conversations. In 2015, Paul Greene, a customer support engineer for SST, testified at a suppression hearing in a Massachusetts criminal case where a recorded conversation was being used as evidence against the defendant.[19] Mr. Greene's testimony revealed several startling facts: (1) ShotSpotter sensors record twenty-four hours a day, seven days a week; (2) each sensor retains seventy-two hours worth of audio recordings; and (3) a conversation at a normal volume may be recorded by a sensor up to fifty feet away. In addition, he estimated that the systems are recording human speech hundreds of times a day. The recordings that were maintained for seventy-two hours were able to be manually searched and then preserved for later use. At the time, SST did not own the recordings and claimed it was not able to prevent its law enforcement customers from searching through audio recordings that were not from gunshots. The NYPD's original contract was for a term of two years starting August 14, 2014.[20] It is not known what the current contract states. Even if the NYPD no longer owns or controls the audio, we do not know whether the NYPD could obtain copies of a non-gunshot recording from SST or if SST would require a court order or a warrant.

Essentially, the ShotSpotter system acts as a massive eavesdropping device[21] that is constantly in use and recording without oversight by the courts. The Legal Aid Society is currently unaware of any case in which the NYPD or a New York City prosecutor obtained an eavesdropping warrant for the use of the ShotSpotter system. Aside from the fact that its utilization violates the fourth amendment and state constitutional rights of citizens, each use of a

---

[19] Transcript from Commonwealth v. Jason Denison, BRC2012-029 (Bristol County Superior Court) (June 12, 2015)
[20] Agreement Between NYPD and ShotSpotter (August 14, 2014)
[21] C.P.L. §700.05(1), P.L. 250.00(2)

ShotSpotter sensor without an eavesdropping warrant may qualify as a class E felony.[22] Unlike the cell-site simulators, the fact that ShotSpotter was being used was not hidden but the breadth of its capabilities were not revealed until later. We still do not know if the NYPD has been accessing, obtaining, or preserving conversations unlawfully recorded by ShotSpotter sensors. We also do not have the NYPD procedures, rules, or guidelines if they exist. Oversight is much needed.

C. Facial Recognition

The NYPD's Facial Identification Section currently operates their facial recognition software. Based upon procurement plans, required to be published under Local Law 63, we believe the NYPD obtained its software from DataWorks Plus. In response to a FOIL request for procedures related to the NYPD's use of facial recognition, from Clare Garvie of the Center on Privacy & Technology at Georgetown University Law Center, the NYPD originally claimed that it was unable to locate any responsive documents.[23] Upon an administrative appeal, the NYPD provided a copy of Chief of Detectives Memo #3 of 2012, but claimed that the remaining responsive documents were exempt under FOIL. An Article 78 proceeding is pending.[24] The Chief of Detectives Memo has limited information on any safeguards used to protect the information used by the Facial Identification Section or where the information is originating from. It also fails to state any mechanisms to avoid false positives or what threshold is required for the program to determine a match.

This is particularly concerning when there is reason to believe that there is a heightened error rate of facial recognition software in the identification of African Americans.[25] While more

---

[22] P.L. 250.05
[23] NYPD Denial of FOIL Request #2016-PL-337 (November 30, 2016)
[24] Center on Privacy & Technology v. NYPD, Index #154060-2017 (N.Y. Co. Supreme Ct. 2017)
[25] Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information, 7 IEEE Transactions on Information Forensics and Security* 1789, 1797 (2012)

research is needed, it appears that facial recognition software in its current state exhibits a racial bias, making it more likely for African Americans to be misidentified.[26] This potential problem is unlikely to be resolved without oversight because the top facial recognition vendors for law enforcement do not test for racial bias.[27] Additionally, false positives are more likely for young adults.[28] Many of the Legal Aid Society's clients are young people of color who already struggle with the biases that exist in the criminal justice system. This additional bias from a secretive software algorithm can be prevented through required procedures and tests.

The lack of guidance for the Facial Identification Section, and the apparent lack of required technical skills to join the unit, have led to a disconcerting practice of manipulating photographs. Adding information or features to photographs or video stills to increase the likelihood of receiving a potential match on the candidate list will increase the number of false positives. While the NYPD can argue that changing the lighting of a picture is acceptable (we do not believe that it is), it is difficult to imagine a scenario in which it would be acceptable to alter a photograph to add eyes when in the original image the subject's eyes were closed. The NYPD has previously used this "technique"[29] among others.[30]

An additional concern is the source of the images provided in the database the NYPD is using. Upon information and belief, we believe the NYPD may be retaining images taken from social media sites in their facial recognition database. We do not know if all of those images were obtained via results from publicly available searches or if they are the result of warrants, court orders, or forcing our clients to turn over social media logins and passwords. There has also

---

[26] Clare Garvie et al., *The Perpetual Lineup: Unregulated Police Face Recognition in America*, Georgetown Law Center on Privacy & Technology at 53-54 (Oct. 2016) (https://www.perpetuallineup.org/)
[27] *Id.* at 55.
[28] Patrick Grother & Mei Ngan, *Face Recognition Vendor Test (FRVT): Performance of Face Identification Algorithms* at 4, 36-38 (May 2014)
[29] "The Art of Facial Recognition" (https://www.forensicmag.com/article/2017/03/art-facial-recognition)
[30] "Behind the Smoking Guns: Inside NYPD's 21st Century Arsenal" (http://creative.nydailynews.com/smokingguns) ("Facial recognition technology requires a face-on image, so the unit used software to create a 3-D, computer-generated image of the shooter's face.")

been a trend for law enforcement agencies across the country to include driver's license photographs in their facial recognition database. At least twenty-six states allow law enforcement to conduct a facial recognition search of their state's driver's license database.[31] If the NYPD is also doing so it would mean that the residents of New York State are routinely being subjected to searches and investigations merely because they have lawfully obtained a driver's license.

If the NYPD has not yet started to use real time facial recognition, it is a potential source of future abuse. The NYPD controls or has access to vast networks of video surveillance that feed into the Domain Awareness System. The new body cameras will be another mass video system. If the NYPD uses these systems with real time facial recognition, it would mean that any person who leaves their apartment may be subject to a database search. And due to the inaccuracies of the technology any person may be falsely seized, which will escalate tensions between many communities and the police, as well as increase overall distrust of law enforcement.

Many of the facial recognition abuses and potential abuses can be prevented by giving the NYPD Inspector General authority to monitor and publicly report on the impact and use of this surveillance technology.

D. Automatic License Plate Readers

The NYPD has set up automatic license plate readers ("LPR") around the city. These readers automatically scan, recognize, and store license plate data. The NYPD keeps this data for five years but it can be extended by the permission of the NYPD Deputy Commissioner of Legal Affairs.[32] These readers and their collected data allow the NYPD to follow individuals via the movements of their vehicles.

---

[31] *The Perpetual Lineup* at 2

[32] Public Security Privacy Guidelines for the Domain Awareness System (4/2/09)

Since at least 2014, the NYPD has had an expanded ability to track individuals all over the country. The agency contracted with Vigilant Solutions who "owns and manages the single largest license plate recognition data sharing initiative (LEARN Database)."[33] Vigilant Solutions bragged in 2014 that it had collected 2.2 billion LPR data records, which were increasing by approximately 100 million new records a month.[34] The addition of this private database to the NYPD's cache of internal databases allows the department to get an even more invasive look into the lives of private citizens. Moreover, officers of the Real Time Crime Center also appear to have access to LPR data collected by the New York State Police, Port Authority Police, Suffolk County Police, and Nassau County Police through the NY/NJ High Intensity Drug Trafficking Area center.[35] It is not clear what LPR information the NYPD makes available to other law enforcement agencies directly or indirectly through Vigilant Solutions. Nor are we aware what procedural safeguards are required of those other groups.

In United States v. Jones[36], The U.S. Supreme Court found that a warrant was required to attach a GPS device to a suspect's vehicle. Justice Sotomayor, in her concurring opinion, acknowledged how intrusive it can be to record an individual's every movement even when those movements are occurring out in the public. But even before Jones, the New York Court of Appeals had already found that such tracking was a violation of one's reasonable expectation of privacy in People v. Weaver.[37] When describing the invasiveness of a GPS tracker the Court stated:

> Disclosed in the data retrieved from the transmitting unit, nearly instantaneously with the press of a button on the highly portable receiving unit, will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center,

---

[33] Agreement Between NYPD and Vigilant Solutions (April 2015)
[34] *Id.*
[35] A heavily redacted copy of NYPD Detective Guide Procedure No. 507-02 received pursuant to a FOIL request by the Legal Aid Society
[36] 132 S.Ct. 945 (2012)
[37] 12 N.Y.3d 433 (2009)

> the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on. What the technology yields and records with breathtaking quality and quantity is a highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious, amicable and amorous, to name only a few—and of the pattern of our professional and avocational pursuits.[38]

While the Court was not addressing LPR, it is clear that the same argument applies. The network the NYPD has created and expanded by private subscription has the capability to expose the private lives of law-abiding citizens. As a result, the potential for its abuse is high and the consequences of such abuse may be great. Oversight and public reporting will curtail this potential for misuse.

CONCLUSION

It is necessary to pass the POST Act to ensure the rights of the citizens of New York City are not violated while still balancing the need for the NYPD to provide effective law enforcement. The Legal Aid Society supports the proposed bill and encourages the City Council to pass it.

---

[38] *Id.* at 441-442