NYPD

Wednesday, June 14, 2017

STATEMENT OF CHIEF ROBERT K. BOYCE
CHIEF OF DETECTIVES
NEW YORK CITY POLICE DEPARTMENT

BEFORE THE NEW YORK CITY COUNCIL
COMMITTEE ON PUBLIC SAFETY
COUNCIL CHAMBERS, CITY HALL
JUNE 14, 2017

Good morning Chair Gibson and members of the Council. I am Chief Robert Boyce, the Chief of Detectives of the New York City Police Department (NYPD). Today I am joined by John Miller, Deputy Commissioner of Intelligence and Counterterrorism, who will also deliver remarks today. Additionally, I am joined here today by Lawrence Byrne, Deputy Commissioner of Legal Matters, and Oleg Chernyavsky, Director of Legislative Affairs. On behalf of Commissioner James P. O'Neill, we are pleased to address the Council today.

At the outset of our testimonies today, I believe it's important to stress that while conducting our sensitive criminal and counterterrorism operations and deploying state-of-the art technology, the value the NYPD places on privacy rights and other constitutional protections is paramount. The protection of civil liberties is as important to the Police Department as the protection of the City itself. **After all, it is these very freedoms that we seek to defend against our adversaries.** Our criminal and counterterrorism investigations are treated with particular care because we recognize that they may, at times, implicate the First and Fourth Amendments and other important issues. Accordingly, we abide not only by the U.S. Constitution and other applicable law, but also, in the case of counterterrorism operations, a federal consent decree that compels additional checks on our investigations. One of our many goals in conducting a criminal investigation is to strike the appropriate balance between public safety with the need to protect privacy rights.

The NYPD Detective Bureau is responsible for the prevention, detection, and investigation of crime, and its efforts often complement the hard work of the police officers assigned to each precinct. Detective work is highly specialized, usually encompassing the examination and evaluation of evidence to apprehend suspects and to build solid cases against them. The Bureau ensures that each one of its commands conducts solid, high-quality investigations in a timely manner and that each investigation is handled efficiently, with dedication and professionalism.

The focus of the hearing today is on surveillance technology utilized by the Police Department. It should be no secret that NYPD investigators are trained to use a variety of technologies. What is important to underscore, however, is that the purpose of using this technology is to prevent, detect, and investigate crime. Where this technology intersects with a legal expectation of privacy, applications for court orders or warrants are made to a District Attorney, which are in turn submitted before a neutral judge. NYPD personnel are trained on how to make these applications. Many of the technologies utilized by our investigators, be it a wiretap, a pen register, a GPS tracking device, or any kind of technology that permits law enforcement to listen to or gain the contents of a communication requires some kind of court-order or warrant.

We do not begin investigations against anything that would be purely constitutionally protected activity. Likewise, we do not conduct surveillance in every case we investigate. Surveillance is not an ominous exercise by local law enforcement – it is routine police work. Our surveillance is triggered out of articulable leads generated from the cases that our personnel are investigating. All of the commands under the Detective Bureau are responsible for ensuring that where legal questions arise in the course of their investigations that personnel confer with the NYPD Legal Bureau, and when appropriate, with the respective District Attorney's Office and the Corporation Counsel to properly resolve any legal issues.

The Fourth Amendment and the State Constitution place a very high burden on law enforcement – and it should be a high burden. This safeguards civil liberties but also ensures that investigations are properly managed and quality arrests are being made. The stakes are too high if we get it wrong.

While Deputy Commissioner Miller will opine more directly on several of the issues with Intro. 1482, I would like to highlight one area. While perhaps in an effort to encompass future technologies, the definition of "surveillance technology" is drafted so broadly that the strict reporting requirements in the bill could be imposed on non-germane technology. For example, by defining surveillance technology as any equipment capable of collecting "location" information, the bill encompasses technology used in our 911 system for emergency response since it is capable of tracking and transmitting location information.

This definition would also encompass important technologies utilized by the Department that protect public safety. This legislation would require the Department to provide an impact and use statement on the Department's Registered Sex Offender and Gun Offender tracking systems. We would be obligated to publically post a detailed description of this technology and its capabilities, thereby revealing the systems potential strengths and limitations to those who would be seeking to exploit this technology or avoid registering altogether. Many other current technologies would be implicated as well, such as our domestic violence incident report tracking system.

I will now turn it over to John Miller, Deputy Commissioner of Intelligence and Counterterrorism, so that he may provide his remarks. Following his remarks, I am happy to take your questions.

NYPD

Wednesday, June 14, 2017

STATEMENT OF JOHN MILLER
DEPUTY COMMISSIONER, INTELLIGENCE AND COUNTERTERRORISM
NEW YORK CITY POLICE DEPARTMENT

BEFORE THE NEW YORK CITY COUNCIL
COMMITTEE ON PUBLIC SAFETY
COUNCIL CHAMBERS, CITY HALL
JUNE 14, 2017

More than any other place in the world, New York City remains in the crosshairs of violent terrorists. Since September 11, 2001, there have been approximately 25 terrorist plots against New York City, with targets such as Times Square, the Brooklyn Bridge, John F. Kennedy Airport, the New York Stock Exchange, the subway system as well as major synagogues and other sites. In most cases, they have been thwarted by the efforts of the NYPD and our local and federal partners. We have been able to build a deterrent that has kept this City safe while protecting and upholding the constitutional rights and liberties accorded to those who live, work, and visit New York City.

September 11th forever changed how the NYPD views its mission and the world around us. Following that tragedy, the Department recognized that we could not defer the responsibility of protecting this City from terrorist attacks to others, and we have continued to prioritize this ever-evolving menace. Soon after 2001, the NYPD became the first police department in the country to develop its own robust counterterrorism capacity. We established a division for training and equipping every one of our police officers for counterterrorism duties. We charged our intelligence operations with a new international focus – our mission now includes gathering and analyzing intelligence with global implications.

Our commitment to ensuring that sufficient resources are dedicated to this critical mission has not changed. One of those premier resources is our personnel. Over the years, the caliber of people we have been able to attract has played a major role in our ability to protect New York. We have hired civilian analysts who are experts in intelligence and foreign affairs. They study terrorist groups, trends, and methods of attacks. Moreover, one of our most important institutional strengths is the remarkable diversity in our ranks. The NYPD is fortunate to have a deep pool of foreign-speaking officers. This has allowed us to build a foreign linguist program with more than 1,200 registered speakers of 85 different languages – Arabic, Dari, Farsi, Mandarin, Pashto, Russian, Spanish, and Urdu, to name just a few. Our diversity has bolstered every aspect of our mission, from counterterrorism to crime-fighting to community relations. Through our Community Affairs Bureau, we have assigned liaisons to the Arab and Muslim, Chinese, Eastern European, Hispanic, and West African communities. They help connect immigrants to needed services and build stronger connections between police and community.

Technology is also critical. In an unprecedented initiative supported by the Department of Homeland Security, we have installed radiation detection equipment throughout neighboring jurisdictions and at key points of entry into the five boroughs so that the City is virtually ringed with an alarm system. This program, called Securing the Cities, includes 150 law enforcement agencies in dozens of nearby cities and towns. The NYPD is responsible for distributing all of the radiation detectors used by our partners.

When it comes to the private sector, we collaborate with nearly 18,000 members of the region's private security industry through a program called NYPD Shield. The membership consists of security

professionals tasked with protecting critical infrastructure and sensitive buildings in the New York metropolitan area. Through the Shield program, we regularly host conferences, sector specific briefings, and training seminars as well as share NYPD strategic assessments on terror trends. Under another initiative, Operation Nexus, our detectives have made visits to businesses that make, sell, or inventory products, services, or materials that might be exploited by terrorists, such as truck rental outfits, fertilizer stores, and chemical supply companies. We ask them to contact us if they see anything unusual, anything that gives them pause.

We also partner with the private sector to secure areas of the City known to be terrorist focal points. We do this through our Domain Awareness System (DAS), a centralized network of security cameras, license plate readers, and chemical and radiological detectors. Using an advanced graphical interface and mapping capability, the DAS is able to retrieve and display information to provide real-time alerts and the means to quickly call up relevant information to guide police action. This makes it possible for us to scan recorded footage for specific objects and behaviors. We can also program the system to alert us to potentially suspicious scenarios: a bag left unattended; a car driving against the flow of traffic, or a person walking through a restricted area. The program receives data from more than 6,600 cameras, nearly 500 license plate readers, and scores of strategically-placed chemical and radiation detectors throughout the City, which provide instant alerts on possible threats in the City. Since it is available as an application on their Department smartphone, the features of the DAS system are available at the fingertips to all of our officers.

Across the City, we have distributed approximately 3,000 radiation pagers to units throughout the department and nearly 4,000 radiological dosimeters to each Patrol Borough's counterterrorism trailer. We continue to invest heavily in acquiring and maintaining state-of-the-art equipment to identify, prevent, or disrupt threats. From sonar systems to thermal imaging cameras, we have installed highly sensitive detection equipment on the boats and helicopters we use to patrol New York Harbor. Police vehicles are also outfitted with similar detection capabilities.

We are also constantly looking to disrupt any budding plots. Every day, through Operation Hercules, we deploy teams of heavily armed officers to make unannounced visits to iconic locations. We stage multiple Critical Response Vehicle deployments throughout the day that proceed in formation, lights flashing, to prearranged locations. We have similar units that focus on ferry terminals, regional transport lines, and the subways.

We place particular emphasis on the subway system in light of its primacy as a target and because it is a vital artery that keeps this City running. In excess of five million New Yorkers use the subways every day. Protecting this system is one of our top priorities and greatest challenges. That is because the entire system is designed to be open, 24 hours a day, every day of the year. Its very strengths as mass transit make it attractive to potential attackers. After the bombing of the London transit system in 2005, we began screening the bags and backpacks of subway passengers. Every day, we maintain posts at each of the 14 underwater subway tunnels. We have heightened uniformed patrols underground and conduct regular security sweeps of subway cars.

These are some of the tools we are using to keep pace with the evolving threat of terrorism. The philosophy behind them is simple: we have to develop the best intelligence available, expand our partnerships, and take protective measures to defeat whatever our adversaries might be planning next.

Unfortunately, our adversaries have multiplied in recent years. What was once the domain of only a few, top-down groups operating from the safe havens of failed or hostile spaces has over time devolved into regional affiliates and local upstarts dispersed across the globe, as well as entrepreneurial lone-wolves within our shores dedicated to actualizing our adversaries' goals.

There have been multiple calls for violence against New York City. In 2014, the 12th issue of *Inspire*, the prominent English-language magazine of al-Qaeda's Yemen-based affiliate, al-Qaeda in the Arabian Peninsula, urged lone-wolf car bomb attacks in U.S. cities, while specifically mentioning the Queens-based U.S. Open as a desirable target. A November Issue of Rumiyah Magazine published by ISIS urged attacks against the Thanksgiving Day Parade. A more recent issue suggested tactics for taking hostages, kidnapping, stabbings and shooting. There are also reports that ISIL and al-Qaeda operatives in Syria and Iraq have continued to plot against the homeland.

In addition to monitoring potential threats from abroad, we have to be concerned about threats originating at home. Last year, we witnessed the horrifying terrorist attack that took place in Orlando, Florida. While I am sure no reminder is necessary, the City itself was the recipient of a terrorist attack through the Chelsea bombing. The attacker had planned this attack for months and took inspiration from Osama bin Laden and other international terrorists.

Last week, two covert operations officers, working on behalf of Hezbollah were charged with undergoing weapons and explosives training and then conducting pre-operational surveillance of potential targets for terrorist attacks including locations in Manhattan, Brooklyn and both airports.

Now, turning to the legislation under consideration today. Intro. 1482 would require the reporting and evaluation of surveillance technologies used by the NYPD. Under this proposal, the Department would be required to issue a surveillance impact and use policy about these technologies and would include information such as its description and capabilities as well as rules, processes and guidelines, and any safeguards and security measures designed to protect the information collected. Upon publication of the draft surveillance impact and use policy, the public would have a period of time to submit comments. The Police Commissioner would have to consider the comments and provide the final version of the surveillance impact and use policy to the Council, the Mayor and post it to the Department's website. Further, the NYPD Inspector General can audit the surveillance impact and use policy to ensure compliance with the bill.

While I will reiterate that the Department is committed to transparency we are also mindful of maintaining the appropriate balance between reasonable transparency and still having the effective tools and technologies needed to protect our city. This proposal would require us to advertise sensitive technologies that criminals and terrorists do not fully understand. It would require the Police Department to list them, all in one place, describe how they work and what the limitations we place on our use of them. In effect, it would make a one-stop-shopping guide for understanding these tools and how to thwart them. The Department absolutely opposes this proposal.

More specifically, this proposal would require the Police Department to provide an impact and use report, and disseminate it online, for each piece of equipment deemed "surveillance technology" and provide a detailed description of the technology and its capabilities. In addition to the examples I provided in my testimony, the tragic events that have taken place today in Alexandria Virginia, and in the United Kingdom over the last several weeks remind us that the threat of terrorism is indeed real and

persistent. A public advertisement detailing the type, quantity, and other specifications of technology and equipment would, report by report, reveal the strengths and potential limitations of the Department's counterterrorism defense operations to any terrorist or criminal organization doing its due diligence. In many ways, producing these reports undermines the security strategy that the technology intends to support.

This is not a passing objection. Terrorists and criminals do their due diligence and they literally study and adapt to evolving security measures. Terrorists and criminals constantly revise their tradecraft to reflect new intelligence. Leaked classified information, publically-available information, and lessons learned from previous operations have provided valuable insight for terrorist groups and criminal enterprises into government surveillance and detection methods. Based on these sources, terrorist groups have been creating formal and informal guidance for would-be followers for years – even before the rise of ISIL.

For example, the "Manchester Papers," also called the "Al-Qaeda Manual," which were discovered in 2000, provided tactical guidance for trained operatives based on knowledge of how law enforcement operates. More recently, ISIL and its supporters have published multiple tactical guides, some with information on specific devices as well as direction on how to evade camera technology.

The recent increased focus on small-scale, low-tech attacks by terrorist organizations is also a response to a greater understanding of how governments disrupt plots. This is the new emphasis by ISIL and other organizations on knife attacks and car-ramming plots. More generally, though, the types of guidance we see – and attacks that have ensued across the Western world recently – are responses to a better understanding of the government playbook writ large.

Terrorist organizations are not the only ones who could exploit this information. Hackers would also welcome this information. Municipal systems have been targeted in the recent past by hackers exploiting security vulnerabilities. This past January, 123 of Washington, DC's 187 Police Cameras were infected with "Ransomware," a malicious software that blocks access to critical data until a ransom is paid. As a result of the attack, the infected cameras were unable to record between January 12 and January 15th. The issue was ultimately resolved by manually removing software from each infected device and restarting the system.

I provide these example because one of the perhaps unintended consequences of the proposed legislation would be that with more knowledge of city systems, vulnerabilities can come to light and be exploited by those seeking to do harm. Anyone looking to conceal activities will exploit vulnerabilities in government programs to design tactics. This legislation would create an effective blueprint for those seeking to do harm.

Other issues also exist with this legislation. The bill requires that the Department disclose in each impact and use statement whether other local, state, federal, or private entities have access to information collected from surveillance technology. We have concerns that publicly disclosing sensitive information such as this could potentially chill our ongoing relationships with our law enforcement partners. Part of this City's success in thwarting potential terror attacks stems from our solid relationship with local, state, and federal partners.

It is also unclear how this legislation is compatible with the state's Freedom of Information Law (FOIL). Producing reports required in this legislation could reveal non-routine investigative techniques, possibly impair present or imminent contract awards, or reveal critical infrastructure. This is all information that is wisely exempted under FOIL.

Furthermore, the bill requires that prior to the use of new technology, the impact and use statement must be posted 90 days in advance and a 45 day period for the public to submit comments to the Police Commissioner must also be permitted for each report. The Police Commissioner is to consider these comments and then finalize this report. The Department is also to amend any impact and use statement when enhancements for current technologies are sought.

This is an unprecedented hurdle placed on a singular agency. Often the technology sought in this legislation is needed imminently and the legislation would impede the Department's ability to evolve critical technology based on changing circumstances.

Proponents of this bill assert that there is a need for this legislation out of concerns for local transparency and oversight. In considering the amount of public reporting conducted by this agency, which is done either voluntary or pursuant to law, as well as the amount of data sets we release each year online, the number of FOIL requests received and responded to, and the fact that our Patrol Guide is now publically available online with minor redactions (pursuant to a bill sponsored by Councilmember Garodnick and supported by the Department), the New York City Police Department is the most transparent municipal police department in the world. Over the last several years, the Department has regularly worked with and negotiated with the Council on a number of pieces of legislation that provide valuable data to the public and the advocacy community. A broad categorization that the Department is not transparent is simply false.

Part of being transparent is to also continually improve trust with communities. For this subject, a particular emphasis is placed on communities most affected by the issues of terrorism. Personnel from our Intelligence and Counterterrorism Bureaus as well as our Community Affairs Bureau regularly meet with religious and community leaders to discuss potential threats, concerning trends, or fears that their communities share.

The exercise of oversight is robust. The court system is indeed providing effective oversight of the NYPD's Intelligence and Counterterrorism initiatives. As you know, the Department operates within the Handschu Guidelines which specifically promulgate how an investigation can be launched and governs the NYPD's investigation of "political" activity, including terrorism-related crimes. Recently, as a result of settling ongoing litigation, the Department has agreed to install a civilian representative on its internal Handschu Committee, which reviews investigations prior to final action by the Deputy Commissioner of Intelligence. This representative, who is former US District Court Judge Stephen Robinson, is appointed by the Mayor and has the ability to review and monitor compliance with all provisions of the Handschu Guidelines. Moreover, the representative is given unfettered access to the courts to communicate any concerns arising out of his function on the Committee.

More locally, the Department is subject to the oversight of the NYPD Inspector General and the City Council. In 2014, I testified before this Committee on the City's emergency preparedness and discussed many of the technologies that would be subject to this legislation. As a Department, we are always willing to engage in substantive discussions with the Council, the advocacy community, and the public

on a variety of topics and it is no secret that representatives from this Department regularly participate in several Council hearings each month.

It would also be an oversight to not mention the very capable work of the attorneys in the Department's Legal Bureau who provide guidance on the constitutionality of specific techniques and whether we are striking the appropriate balance between security concerns and civil liberties. The NYPD's Legal Bureau has several attorneys specifically assigned to handle intelligence and counterterrorism issues and the Deputy Commissioner of Legal Matters plays a vital role on our Handschu Committee.

While legislation similar to this proposal has been enacted in other jurisdictions, it is fair to say that none of these jurisdictions are the number one target of terrorism worldwide. That is not speculation – it is the consensus of the global intelligence community.

Furthermore, although federal agencies are obligated to submit privacy impact assessments on their information technology pursuant to the E-Government Act of 2002, these federal requirements are distinguishable from the bill under consideration today. Most notably, federal law does not require publicizing privacy impact assessments for technology and systems which involve, among other things, sensitive information that could potentially damage law enforcement efforts or raise security concerns.

Federal law requires impact assessments throughout multiple federal agencies and encompasses systems and equipment used throughout the country. This bill focuses on one agency and essentially is so localized that it provides a particularized list of the critical technology and equipment used to defend and protect a single jurisdiction.

In the final analysis, all that this legislation does is provide an invaluable roadmap to terrorists, criminals, and others on how to more effectively harm the public, commit crimes, and hurt the interests of our City.

Over fifteen years after 9/11, New York enjoys the distinction of being the safest big city in America. It is also commercially vibrant, culturally diverse, and free. We can claim these successes are due, in no small measure, to the 50,000+ uniformed and civilian members of the New York City Police Department, in cooperation with our local, state, and federal partners, who have demonstrated initiative and perseverance in the face of varied and continuing threats.

Thank you again for this opportunity to testify today. I am happy to answer any questions you may have.

DANIEL R. GARODNICK
COUNCIL MEMBER, DISTRICT 4

DISTRICT OFFICE:
211 E. 43RD ST., SUITE 1205
NEW YORK, NY 10017
TEL: (212) 818-0580
FAX: (212) 818-0706

CITY HALL OFFICE:
250 BROADWAY, ROOM 1762
NEW YORK, NY 10007
TEL: (212) 788-7393
FAX: (212) 442-1457

THE COUNCIL
OF
THE CITY OF NEW YORK

CHAIR

ECONOMIC DEVELOPMENT

COMMITTEES

LAND USE
EDUCATION
TRANSPORTATION
WATERFRONTS
RULES, PRIVILEGES &ELECTIONS
ZONING & FRANCHISES

Remarks of Council Member Daniel R. Garodnick
Before the Committee on Public Safety
Regarding Intro 1482: The Public Oversight of Surveillance Technology (POST) Act
June 14, 2017

Thank you Chair Gibson for holding a hearing on Intro 1482 or the POST Act, which I introduced along with the Chair. The POST Act would require the New York City Police Department to publicly disclose on its website impact and use policies about surveillance technologies it is currently using and plans to use in the future. These policies must be posted for public comment within 90 days of use of a new technology, with comments accepted for 45 days, and final drafts of the policies posted no more than 45 days after the comment period closes.

The NYPD has, and should continue to have an impressive capability for surveillance. We live in uncertain times and surveillance is critical to their operations and for keeping New Yorkers safe. But civilians are in charge of the police force, and we need to be able to understand what technologies are used in our name. Unfortunately, surveillance technologies are too often not only used in secret, but also acquired in secret. Even local elected officials like us are kept in the dark about what technologies the NYPD is buying and how they are being used. A disclosure process for surveillance technology would foster more public trust in our law enforcement system.

The POST Act would require the NYPD to make clear how they plan to use any new surveillance technology, and to accept feedback on its plans. It would give the public a chance to engage substantively with the NYPD's decisions regarding surveillance, and that public feedback may actually help to expose weaknesses or shortcomings in PD's approach. And public awareness of NYPD capabilities may also deter would-be terrorists and criminals in the same way as does an officer's physical presence on the street. It would also help reassure New Yorkers that the city has sufficient safeguards in place for sensitive information in an era of increasing hacks and data breaches. Finally, the POST Act reinforces our commitment as a Sanctuary City by requiring the NYPD to disclose if any outside entities -- including the state or federal governments -- have access to data collected by local surveillance technology.

What this bill does not do is impact the ability of our police to use this technology. We carefully crafted the bill so that it does not require the NYPD to disclose operational details regarding when and where it will employ a specific tool.

Let's face it -- people always learn about police surveillance tools, eventually. This bill gives the chance for the public to engage with and even embrace this technology. And it gives the police the chance to re-examine their policies before everything gets revealed in bits and pieces.

This law represents the best thinking for modern policing. I look forward to hearing today's testimony, and I urge my colleagues to support this bill, and bring some real reform to covert surveillance in our city.

THE LEGAL AID SOCIETY

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

https://www.privacyboard.nyc

Honored members of the City Council,

We are the NYC Privacy Board Advocates (#NYCPrivacy). We advocate for the creation of a Privacy Guidelines Board to advise city legislators and agencies in the creation of policies that will protect New Yorkers' data from being misused.

#NYCPrivacy supporters demand that the city create strong policies and oversight to keep pace with a torrent of new technologies which have the potential for unintended disclosure of individual's' data. We feel that the POST Act works toward our vision.

The POST Act allows citizens to consider and influence how those technologies are used in society. With such consideration and voice, it allows New Yorkers to proactively limit unintended consequences and prepare us to handle them.

The growing power of technologies and how they integrate into society must be matched by a proportionate responsibility for how they are used.

Sincerely

TESTIMONY OF CHAD A. MARLOW, ACLU ADVOCACY & POLICY COUNSEL, IN SUPPORT OF INTRO. 1482

JUNE 14, 2017

Madam Chair and Members of the Public Safety Committee, my name is Chad Marlow and I am an Advocacy and Policy Counsel at the American Civil Liberties Union. I am pleased to appear before you today to offer the ACLU's strong endorsement of Intro. 1482 – the POST Act.

Many others here today will touch upon the importance of the POST Act in promoting government transparency and greater public involvement in decisions regarding law enforcement use of surveillance technologies. They will properly highlight how these technologies threaten New Yorkers' civil liberties, but that they threaten some communities far more than others. When the ACLU has been able to peer behind the veil of secrecy that has been thrown over the use of these technologies, we have consistently found – from Milwaukee, Wisconsin to Tallahassee, Florida, and from Baltimore, Maryland to Oakland, California – that they are overwhelmingly deployed against communities of color, making them a threat to civil rights as well as to civil liberties. All of these facts support New York City adopting the POST Act, but to avoid redundancy, I instead would like to focus on two other points.

The first is simply to state that in taking up the POST Act, New York City is far from acting alone. The POST Act is a part of a nationwide movement to promote greater government transparency and community input into decisions involving the acquisition and use of surveillance technologies. In considering the POST Act, New York City joins 18 other American cities where similar legislation has already been introduced or has a sponsor who is preparing to introduce it. A version of this bill is also being considered by the State of Maine and by the Bay Area Rapid Transit system in California, which is roughly the equivalent of the MTA in New York City. Grassroots efforts to secure bill sponsors are also underway in more than 40 additional American cities. And presently, public oversight of surveillance technology laws are already on the books in Seattle, Washington and in Santa Clara County, California, the home of Silicon Valley. So lest you be told otherwise, the POST Act is not an isolated or unusual measure – it is part of a national movement, and I congratulate the New York City Council for its engagement in that effort. Of course, to truly protect New Yorkers and to become a national leader in this movement, New York City needs to pass the POST Act into law.

But most importantly, I am here to talk to you about a question the POST Act raises that should be on every City Council Member's mind as they weigh whether to support this measure;

namely, are you committed, truly committed, to doing everything in your power to prevent President Donald Trump from pursuing his illegal and unconstitutional agenda in New York City? Because that is what the POST Act will help our city do. Let me explain.

When Donald Trump ran for President, he told the American public, repeatedly, that upon taking office he would focus his efforts on identifying and deporting millions of undocumented immigrants, on tracking and surveilling Muslims throughout the country and banning their travel to this country, and on promoting even more aggressive policing against communities of color. Say what you will about the President, at least in this regard, he has been a man of his word.

But here is an important wrinkle worth noting: President Trump needs more personnel than are available to him on the federal level to execute these policies, which involve targeting millions of people nationwide and hundreds of thousands of people right here in New York City. Trump needs to enlist the help of local law enforcement, and he has been trying to do just that. Case in point, on January 25, 2017, President Trump signed an executive order reviving "programs that allow the federal government to work with local and state law enforcement agencies . . . to share information to help track and deport [immigrants]."

Now we know the voluntary help Trump needs is not going to be forthcoming in New York City. The Mayor has promised us the NYPD will not actively assist Trump in pursuing his agenda, and we are grateful for that. The Mayor and this Council have proudly declared New York to be an open and welcoming city, a safe city, a sanctuary city, but that is not enough. While New York City has posted guards at its front door to prevent Trump from going after immigrant, Muslim, and other targeted communities, the city has left no one guarding its back door.

What is that back door? It is law enforcement providing passive, secret assistance to Trump by giving him access to NYPD surveillance data. How does this work exactly? By the Trump administration continuing and expanding upon existing Obama-administration programs that have offered millions of dollars in grants to local police forces to purchase surveillance technologies.

The grants work like this: the federal government agrees to pay for a local police department's surveillance technology in exchange for sharing the information it collects. Such a secret deal might even include the feds receiving real-time access to video and audio feeds. This means if the NYPD uses a Trump-surveillance grant to purchase a Stingray cell-site simulator, when that device captures location data from thousands of cell phones, the Trump administration may be able to directly or indirectly access that data and use it to locate and track immigrants and Muslims. Or if the NYPD uses the grant money to purchase and install surveillance-enabled lightbulbs, President Trump's federal agencies may be able to access their live and recorded video and audio feeds and use them to spy on communities of color and neighborhoods with high Muslim or foreign-born populations. This is not science fiction – it is science fact. Just last month it was revealed that ICE used a Stingray to locate an undocumented immigrant in

Michigan. And in Oakland, California, Brian Kofer, the chair of that city's Privacy Advisory Commission, stated that his Commission "has a paper trail" showing that ICE has been accessing the Oakland Police Department's automatic license plate reader data. Oakland, incidentally, is also a sanctuary city.

Does the NYPD have such data sharing agreements with the federal government? Is it considering accepting grants that will create or expand such data sharing programs? You, the Members of the City Council of New York, have no idea. The public you represent has no idea. And by keeping us in the dark, the NYPD has deprived us of our ability to speak out against such agreements when they are being contemplated.

The NYPD can do this legally because, right now, it has the unchecked authority to decide, in secret, when and under what terms it acquires and uses surveillance technologies, and with whom it shares surveillance technology data and access. The only way to change that practice is to change the law. That is what the POST Act is all about.

Instead of allowing the NYPD to secretly and unilaterally approve the acquisition and use of surveillance technologies, the POST Act would require the NYPD to provide information about proposed acquisitions and uses to the Council and the public so we are empowered to raise objections with the Mayor and NYPD. And this not only goes for newly acquired technologies, but for ones currently in the field, and it covers data sharing agreements.

In short, the POST Act, if adopted, would undermine the Trump administration's ability to secretly use NYPD surveillance technologies to spy on the public. The POST Act will keep New York City's residents and visitors safe from the real and serious threats that are emanating from the White House. You want to know what the resistance looks like? The POST Act is what it looks like.

Now I know that many members of this Council have spoken out against Trump's targeting of immigrants, Muslims, and other communities, and we are very grateful for that. But now, with the POST Act before you, we have arrived at a critical moment. This is a real opportunity, for all of us, to show how committed we truly are to making New York a city where everyone is welcome and everyone is safe. Words are not enough to keep people safe. Action is required, and now is a time for action.

The ACLU respectfully requests you support the adoption of the POST Act in New York City.

RESTORE the FOURTH

THE FOURTH AMENDMENT

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

June 13, 2017

Honored members of the City Council,

We are a national civil liberties organization urging you to adopt the POST Act. We fully endorse the comments presented by NYCLU and would like to add a few remarks regarding the ways in which this legislation would restore the protections embodied in the Fourth Amendment of our Constitution.

The Fourth Amendment protects US residents from searches and seizures without probable cause. It requires transparency by emphasizing the role of independent external review before law enforcement conduct searches and seizures. When it comes to technology, from stingrays to drones to X-ray vans, the NYPD has tried very hard to hide its technology from any external review-- from the equipment they acquire to the surveillance they conduct. It is high time for that to change.

Passing the POST Act would finally require the NYPD to develop policies for deploying a new technology *before* its deployment and it would give you, member of the council, a role in assessing it for reasonability. We expect these policies will specify whether a warrant will be required and whether incidentally gathered data can be retained for use in future investigations.

It's easy for new surveillance technologies to turn into dragnets; the POST Act creates a mechanism for preventing such dragnets and it places the responsibility in the most appropriate hands-- the city council--with our democratically elected officials, along with the input of people who attend and testify at a public hearing such as this one.

We care desperately about the Fourth Amendment and see it under increasing threat. A public review process for surveillance technologies will allow for discussion and debate informed by the perspectives of elected officials, the general public and technology experts, and not just the perspectives of law enforcement.

That's a balance we sorely need.

Sincerely,

Alex Marthews, National Chair, Restore The Fourth
Theo Chino, Restore The Fourth – NYC.

Mailing address: 28 Temple St., Belmont, MA 02478 ~ 781-258-2936 ~ www.restorethe4th.com ~ @Restore_The4th

Testimony of Harlan Yu
Principal, Upturn

New York City Council
Committee on Public Safety

Hearing on
Creating Comprehensive Reporting and Oversight
of NYPD Surveillance Technologies
Int. No. 1482

June 14, 2017

Good morning, Chairperson Gibson and members of the Committee on Public Safety. My name is Harlan Yu and I am a Principal at Upturn. We work with local and national civil rights groups on issues where technology meets policing. For the last two years, we've been focusing on body-worn cameras.

Body-worn cameras are powerful surveillance tools. Whether or not cameras ultimately hold the police more accountable, cameras will intensify surveillance in New York communities — especially in many communities of color, where officers and cameras will be most rampant. In a set of Civil Rights Principles on Body-Worn Cameras, a major coalition of civil rights and privacy groups warned that "there is a real risk that these new devices could become instruments of injustice, rather than tools for accountability."[1]

We need not only strong policy safeguards, but also transparency and continued public oversight to ensure that cameras will serve the interests of New York's residents — and that's what the POST Act would help to provide.

The POST Act would require annual IG audits of body camera use, to help ensure on an ongoing basis that officers are turning their cameras on and off when they're supposed to, and that footage is retained, secured and accessed according to the department's policy.

Strong public oversight is all the more important for fast changing technologies, like body-worn cameras. Right now, VIEVU, the vendor which supplies cameras to the NYPD, is building face recognition and other automated search capabilities into their system.[2] This could give the NYPD the power to automatically scan and search every face that a body camera sees, and would quickly turn body cameras into a system of intense, localized mass surveillance.

---

[1] The Leadership Conference on Civil and Human Rights, *Civil Rights, Privacy, and Media Rights Groups Release Principles for Law Enforcement Body Worn Cameras* (May 15, 2015), http://www.civilrights.org/press/2015/body-camera-principles.html.

[2] *Vievu and Veritone to Bring Artificial Intelligence to LE Audio and Video Data*, POLICE Magazine (Apr. 12, 2017), http://www.policemag.com/channel/technology/news/2017/04/12/vievu-and-veritone-to-bring-artificial-intelligence-to-le-audio-and-video-data.aspx.

Even though the NYPD's body camera program is subject to some judicial oversight through *Floyd*, that is no substitute for what the POST Act would require. In particular, Judge Torres only has jurisdiction over the NYPD's one-year *pilot* program — after the first year, the NYPD could incorporate face recognition into their body cameras without telling the judge, or the public.

These powerful new capabilities should not be adopted in secret. The POST Act would provide the public with meaningful safeguards, without compromising public safety. It would simply require the NYPD to explain how it intends to use the technology, and give New Yorkers a chance to weigh in. The POST Act is a balanced and common sense proposal that would shed important light on the NYPD's most invasive practices.

BRENNAN
CENTER
FOR JUSTICE
TWENTY
YEARS

Brennan Center for Justice
at New York University School of Law

120 Broadway
Suite 1750
New York, New York 10271
646.292.8310 Fax 212.463.7308
www.brennancenter.org

June 14, 2017

Written Testimony of Michael Price, Counsel
Brennan Center for Justice at New York University Law School
Before the
New York City Council Committee on Public Safety
In Support of Int. 1482

Good afternoon, Chairwoman Gibson and members of the Public Safety Committee. My name is Michael Price and I serve as Counsel for the Brennan Center for Justice at NYU School of Law in the Liberty and National Security Program. Thank you for holding this hearing and inviting the Brennan Center to testify in support of Int. 1482, the Public Oversight of Surveillance Technology Act. And thank you once again to Councilmembers Daniel Garodnick and Vanessa L. Gibson for co-sponsoring this important reform.

The Brennan Center is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. The Liberty and National Security Program focuses on helping to safeguard our constitutional ideals in the fight against terrorism. As a part of that work, we advocated for the creation of an Inspector General for the NYPD in 2013, following the NYPD's well-documented and unconstitutional surveillance of Muslim communities. And we continue to seek greater transparency and oversight of NYPD surveillance practices, including the use of powerful new technologies that present profound concerns for civil rights and civil liberties, now more than ever. That is why the Brennan Center is proud to support the POST Act here today.

The Brennan Center commends the Council on its thoughtful approach to balancing the need for democratic oversight and transparency with the NYPD's legitimate need for operational secrecy. Although the NYPD may not wish to discuss the surveillance tools they use, a strong local democracy like New York City requires at least a basic level of information about what its local police are doing and how they're doing it. The POST Act will inform the public – and critically, members of the City Council – about the kinds of information the NYPD collects and the policies in place for retaining, sharing, and protecting it. It also carefully avoids the disclosure of operational details that might compromise police investigations or harm public safety.

Specifically, the bill would require the NYPD to create an "impact and use policy" for surveillance technologies now in use as well as any new technologies that come along in

the future. The requirement would cover devices like "Stingrays" (cell phone locators),[1] automatic license plate readers,[2] and mobile "X-ray" vans.[3] It would also include software like automated facial recognition programs[4] as well as information sharing networks like the $40 million Domain Awareness System, which combines information from NYPD records and databases with the thousands of public and private security cameras that blanket the city.[5] Reports would have to describe what the technology does as well as the policies and procedures for using it, like whether a warrant or court order is necessary. They would also describe the rules for using or sharing[6] the information collected as well as safeguards to prevent unauthorized access, whether training is required, and any internal compliance procedures.

Such information is essential to effective public oversight, but it is too general to be a tool for those who might wish to evade lawful police surveillance. It does not provide any information about how the NYPD uses the technology in connection with specific investigations or types of investigations. It does not disclose where or when it might be used or how someone might defeat it. It also does not make the tools any less effective. Wiretaps, for example, remain a potent investigative tool despite widespread knowledge of their existence and the strict rules for their use. Likewise, Stingrays will continue to work; X-ray vans will continue to see through cars and buildings, and license plate readers will continue to read license plates. Unless criminals and terrorists stop using cell phones and cars, these devices will be just as effective as they are today.

It is true that the NYPD might enjoy a brief advantage if it were to secretly acquire a new technology that is completely unknown to the public. But history shows that the public inevitably finds out, through costly Freedom of Information Law (FOIL) litigation, through the press, or through the courts. Indeed, law enforcement has an obligation to properly disclose information about its use of surveillance technologies to judges and

---

[1] Reuven Blau, "Here's how the NYPD's Stingray tech can spy on New Yorker's cell phones," *New York Daily News*, March 9, 2017, http://www.nydailynews.com/new-york/nypd-stingray-tech-spy-new-yorker-cell-phones-article-1.2992708.

[2] Mariko Hirose, "Documents Uncover NYPD's Vast License Plate Reader Database," *American Civil Liberties Union* (blog), January 25, 2016, https://www.aclu.org/blog/free-future/documents-uncover-nypds-vast-license-plate-reader-database.

[3] Conor Friedersdorf, "The NYPD Is Using Mobile X-Ray Vans to Spy on Unknown Targets," *Atlantic*, October 19, 2015, https://www.theatlantic.com/politics/archive/2015/10/the-nypd-is-using-mobile-x-rays-to-spy-on-unknown-targets/411181/.

[4] Claire Garvie and Alvaro Bedoya, "Smile! You've just been identified by face recognition," *New York Daily News*, March 27, 2017, http://www.nydailynews.com/opinion/smile-identified-face-recognition-article-1.3008512.

[5] Joe Coscarelli, "The NYPD's Domain Awareness System Is Watching You," *New York Magazine*, August 12, 2012, http://nymag.com/daily/intelligencer/2012/08/nypd-domain-awareness-system-microsoft-is-watching-you.html.

[6] The POST Act specifically requires the NYPD to disclose whether it shares data with outside agencies at the state and federal level. This is a critical feature of the bill that would assist New Yorkers in understanding how the NYPD shares information. Unfortunately, it does not require sufficient particularity regarding *which* federal agencies receive data. New Yorkers should know, for example, what data is being shared with ICE, directly or indirectly. The Brennan Center therefore recommends a more granular approach to Section 1(a)(6) that would require the NYPD to indicate which federal and state agencies are receiving or have access to NYPD data.

criminal defendants. The failure to do so can jeopardize thousands of investigations, as was the case in Maryland and Florida when investigators concealed their use of Stingrays from the courts by referring to them as a "confidential source."[7] Thus, even without this law, it is wishful thinking to suppose that the NYPD's surveillance tools would remain a secret for very long. The real question is when, not whether, the NYPD will need to acknowledge its use of new technologies.

The goal of the POST Act is to front-load that discussion, to have an informed conversation with policymakers and community stakeholders about the rules of the road *before* the NYPD deploys a new technology and *before* there is another alarming headline about police surveillance. Such a proactive approach provides an opportunity for up-front, constructive community input. It also encourages the NYPD to be thoughtful in how it approaches new surveillance technologies, so as not to engage in activities that harm individual rights, undermine its relationships with communities, or waste scarce resources.

This is a common sense idea embraced by law enforcement leaders. In 2015, President Obama's Task Force on 21st Century Policing specifically recommended that state and local law enforcement agencies "encourage public engagement and collaboration … when developing a policy for the use of a new technology."[8] According to the final report: "Local residents will be more accepting of and respond more positively to technology when they have been informed of new developments and their input has been encouraged. How police use technology and how they share that information with the public is critical."[9] Task Force co-chair Charles Ramsey also recognized that, "Just having the conversation can increase trust and legitimacy and help departments make better decisions."[10]

In fact, the federal government routinely discloses its ground rules for using new technologies. For example, both the Department of Justice[11] and the Department of Homeland Security[12] (DHS) have published policies on their use of Stingrays, requiring

---

[7] Nicky Wolf, "2,000 cases may be overturned because police used secret Stingray surveillance," *Guardian*, September 4, 2015, https://www.theguardian.com/us-news/2015/sep/04/baltimore-cases-overturned-police-secret-stingray-surveillance; Kim Zetter, "Emails Show Feds Asking Florida Cops to Deceive Judges," *Wired*, June 19, 2014, https://www.wired.com/2014/06/feds-told-cops-to-deceive-courts-about-stingray/.

[8] President's Task Force on 21st Century Policing, *Final Report od the President's Task Force on 21st Century Policing* (Washington, DC: Office of Community Oriented Policing Services, 2015), 35, https://cops.usdoj.gov/pdf/taskforce/taskforce_finalreport.pdf.

[9] Ibid.

[10] Ibid; *see also Privacy impact assessment report for the utilization of license plate readers* (Alexandria, VA: International Association of Chiefs of Police, 2009), 28, http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf. (recognizing that "[o]ne way to promote public confidence is to increase the transparency surrounding how [license plate reader] data will be managed by the law enforcement agency.").

[11] U.S. Department of Justice, *Department of Justice Policy Guidance: Use of Cell-site Simulator Technology*, https://www.justice.gov/opa/file/767321/download (accessed June 13, 2017).

[12] Alejandro N. Mayorkas, Memorandum to Sarah Saldana, et al., "Department Policy Regarding the Use of Cell-Site Simulator Technology," October 19, 2015, https://www.dhs.gov/sites/default/files/publications/Department Policy Regarding the Use of Cell-Site Simulator Technology.pdf.

agents to obtain a judicial warrant and apply important back-end privacy protections. DHS has also publicly described its use of backscatter x-ray systems for border security; issued Privacy Impact Assessments for use of facial recognition technology[13] and license plate reader data;[14] and issued guidance for state and local agencies using drones, which strongly recommended transparency and public outreach.[15] If the two federal agencies responsible for protecting our domestic national security can provide this type of information to the general public, then the NYPD can surely do so as well.

The NYPD may also discover that there are benefits to community engagement, as in Oakland, California, where police officials say they have helped build community trust through transparency and dialogue on surveillance technology issues.[16] Oakland police have already begun to implement an ordinance, widely expected to become law, which contains transparency reporting requirements comparable to the POST Act.[17] In preparation, police officials have begun attending public oversight meetings to provide information about the different surveillance technologies that Oakland uses, including Stingrays, and the privacy concerns they raise.[18] From a police perspective, sharing this information has helped build community relationships and trust where there was little before. Tim Birch, a former Oakland police officer and current head of the Oakland Police Department's Research and Planning team, now considers it "bizarre" that there is "a world in which we don't want the public to know what we are doing or what we are doing with it. What equipment we have or how we are using it."[19] In New York, by contrast, the NYPD has been secretly using Stingrays for years, and yet the Department continues to fight FOIL requests for information about how it uses the devices.[20]

---

[13] U.S. Department of Homeland Security, U.S. Customs and Border Protection, *Privacy Impact Assessment for the Facial Recognition Air Entry Pilot*, DHS/CBP/PIA-025 (March 11, 2015), https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp-1-to-1-facial-recognition-air-entry-pilot-march-11-2015.pdf (accessed June 13, 2017).

[14] U.S. Department of Homeland Security, U.S. Immigrations and Customs Enforcement, *Privacy Impact Assessment for the Acquisition and Use of License Plate Reader Data from a Commercial Service*, DHS/ICE/PIA-039 (March 19, 2015) https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-lpr-march2015.pdf (accessed June 13, 2017) .

[15] U.S. Department of Homeland Security, Privacy, Civil Rights & Civil Liberties Unmanned Systems Working Group, *Best Practices for Protecting Privacy, Civil Rights & Civil Liberties Liberties in Unmanned Systems Programs* (December 18, 2015), https://www.dhs.gov/sites/default/files/publications/UAS%20Best%20Practices.pdf (accessed June 13, 2017).

[16] Michael Price, "What Oakland police can teach the NYPD," *amNewYork* (blog), May 12, 2017, http://www.amny.com/opinion/what-oakland-police-can-teach-the-nypd-1.13624678.

[17] Oakland, Cal., The Surveillnace and Community Safety Ordinance (Jan. 5, 2016), *available at* https://www.documentcloud.org/documents/3253520-oak061975.html (Draft).

[18] "Privacy Advisory Commission – LIVE," City of Oakland video, from a city council meeting televised on August 11, 2016, http://oakland.granicus.com/MediaPlayer.php?publish_id=0891cb33-63f2-11e6-8170-f04da2064c47

[19] Cyrus Farivar, "Ex-Cop: it's 'bizarre' if we can't explain to public what our snooping gear does," *Ars Technica*, January 29, 2017, https://arstechnica.com/tech-policy/2017/01/how-an-ex-cop-tries-to-get-a-police-department-to-think-about-privacy/.

[20] Barbara Ross, "NYCLU sues the NYPD to get Stingray spyware info," *New York Daily News*, May 19, 2016, http://www.nydailynews.com/new-york/nyclu-sues-nypd-stingray-spyware-info-article-1.2643103.

New Yorkers all want the NYPD to keep New York City safe, but new surveillance technologies do not just capture information about the "bad guys." They affect the privacy rights of all New Yorkers, especially – and disproportionately – communities of color. Without some basic information about what these technologies do and how the NYPD is using them, lawmakers and government watchdogs, including the NYPD Inspector General, cannot oversee the NYPD or do their jobs effectively.

Transparency and oversight are essential features of a strong democracy, and the Brennan Center commends the Council and this Committee for addressing this critical and timely issue. The Brennan Center strongly supports Int. 1482 and we encourage the Council pass it quickly.

Thank you again for the opportunity to testify today. I am happy to answer any questions.

CAIR NEW YORK

Council on American-Islamic Relations

46-01 20th Avenue
Astoria, New York 11105

www.cair-ny.org | (646) 665-7599

STATEMENT OF
ALBERT FOX CAHN, ESQ.
LEGAL DIRECTOR
COUNCIL ON AMERICAN-ISLAMIC RELATIONS, NEW YORK, INC.

BEFORE THE
COMMITTEE ON PUBLIC SAFETY
NEW YORK CITY COUNCIL

FOR A HEARING CONCERNING,
CREATING COMPREHENSIVE REPORTING AND OVERSIGHT OF NYPD SURVEILLANCE TECHNOLOGIES

PRESENTED
June 14, 2017*

* My sincerest thanks to Steven Demarest, CAIR-NY Civil Rights Intern, for his invaluable assistance in preparing these remarks.

Good morning, my name is Albert Fox Cahn, and I serve as the Legal Director for the New York Chapter of the Council on American-Islamic Relations ("CAIR-NY"). CAIR-NY is a leading civil rights advocacy organization for the Muslim community here in New York City and across New York State. I speak today in support of the POST Act, which would be an important step forward in strengthening police oversight, promoting public safety, and safeguarding New Yorkers' privacy rights.

Historically, the New York City Police Department ("NYPD") deployed novel and highly invasive surveillance technologies in ways that circumvented democratic oversight and accountability. The NYPD used private and federal funds, without any disclosure to the lawmakers we depend-on to oversee our police forces. With this unaccountable funding, the NYPD was able to deploy tools like "stingrays," fake cell towers that collect sensitive location and communications data.[1] Like many of the NYPD's new tools, stingrays spy not only on the target of an investigation, but also on untold numbers of innocent bystanders.[2]

Let me be clear, the POST Act does not prohibit the NYPD from using new surveillance tools. Rather, it merely secures this Council's indispensable role in reviewing when and how such tools are deployed. Under the POST Act, the NYPD must issue an "impact and use policy" report when choosing to use a new surveillance tool.[3] This report must describe the technology, rules, and guidelines for the use of that technology, and safeguards for protecting any data collected.[4] The City Council and the people of New York City would then be allowed to provide feedback on such an acquisition.[5] Thuse, the POST Act strikes a delicate balance, requiring sufficient information to ensure oversight, while protecting operational details, sources, and methods.

Civilian oversight of policing and intelligence gathering is not only a fundamental American value, it is essential for effective policing. As then-President Obama's Task Force on 21st Century Policing found, "[l]aw enforcement agencies should establish a culture of transparency and accountability in order to build public trust and legitimacy."[6] The NYPD's current procurement methods are not only undemocratic, but they harm the NYPD's very mission of promoting public safety.

---

[1] Joseph Goldstein, *New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says*, N.Y. TIMES, Feb. 11, 2016, https://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html.

[2] *Id.*

[3] N.Y. CITY COUNCIL 1482 § 1 (N.Y. 2017), ch. 1, 14 ADMIN. CODE OF N.Y.C. § 14-167(b) (as proposed)

[4] *Id.* at 14-167(a) (as proposed)

[5] *Id.* at 14-167(e-f) (as proposed)

(Cont'd on following page)

The POST Act will benefit all New Yorkers, but it will offer particularly powerful protection for our Muslim neighbours. For years, Muslim New Yorkers have faced a pattern of unjust and unconstitutional NYPD surveillance. Specifically, the NYPD's Intelligence Division engaged in extensive, suspicionless surveillance of majority Muslim neighbourhoods and Muslim families.[7] Additionally, NYPD officials have conducted blanket surveillance of entire mosques, surveilling men, women, and children for nothing more than practicing their faith.[8] Some local businesses have even been classified as "place[s] of concern" for nothing more than having customers of middle eastern dissent.[9]

In addition, Muslim New Yorkers who opened their doors to law enforcement, hoping to help their community, frequently were rewarded with suspicion and surveillance. In one example, Sheikh Reda Shata welcomed FBI agents and NYPD officers into his mosque, trying to build a bridge between the community and law enforcement, but was nonetheless monitored by an undercover police officer.[10]

Muslim New Yorkers who are targeted for their faith often self-censor or pull back from their religious practices. Although most Muslim New Yorkers continue to unapologetically practice their faith in the face of police harassment, some have stopped attending their places of worship.[11] Those who continue to attend services face frequently insurmountable barriers to building trust with those around them, knowing that a friendly co-congregant may secretly be an undercover officer.[12] Other

(Cont'd from preceding page)

[6] PRESIDENT'S TASK FORCE ON 21ST CENTURY POLICING, FINAL REPORT OF THE PRESIDENT'S TASK FORCE ON 21ST CENTURY POLICING 12 (2015), https://cops.usdoj.gov/pdf/taskforce/taskforce_finalreport.pdf.

[7] Matt Apuzzo & Joseph Goldstein, *New York Drops Unit That Spied on Muslims*, N.Y. TIMES, Apr. 15, 2014, https://www.nytimes.com/2014/04/16/nyregion/police-unit-that-spied-on-muslims-is-disbanded.html?_r=0; *see also* DIALA SHAMAS & NERMEEN ARASTU, MUSLIM AM. CIVIL LIBERTIES COAL., CREATING LAW ENF'T ACCOUNTABILITY & RESPONSIBILITY & ASIAN AM. LEGAL DEF. & EDUC. FUND, MAPPING MUSLIMS: NYPD SPYING AND ITS IMPACT ON AMERICAN MUSLIMS 10 (2013), https://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

[8] Apuzzo & Goldstein, *supra* note 7.

[9] Adam Goldman & Matt Apuzzo, *NYPD: Muslim Spying Led to No Leads, Terror Cases*, ASSOCIATED PRESS, Aug. 21, 2012, https://www.ap.org/ap-in-the-news/2012/nypd-muslim-spying-led-to-no-leads-terror-cases.

[10] Eileen Sullivan, *NYPD Spied on Anti-terror Muslim Leader as He Dined with Bloomberg*, NBC NEWS, Oct. 6, 2011, https://www.nbcnews.com/id/44796663/ns/us_news-life/t/nypd-spied-anti-terror-muslim-leader-he-dined-bloomberg/.

[11] SHAMAS & ARASTU, *supra* note 7, at 12-14.

[12] *Id.* at 18.

New Yorkers are afraid to practice their faith as they'd wish, refraining from wearing a beard, a headscarf, or other visible signifiers of their religion.[13] Moreover, Muslim faith leaders often speak guardedly to their congregations, fearful that an out-of-context statement, or even speaking a disfavoured dialect, might spark an investigation.[14]

Muslim student groups have also faced widespread and discriminatory surveillance. New York's Muslim Student Associations have been targeted with informants and undercover officers for as little as organizing a rafting trip[15] or having members deemed "politically active."[16] One reason why the POST Act is so crucial is that many of the most invasive NYPD programs have never produced a single lead, let alone stop a terrorist act.[17] Yet these same technologies and tactics, whose rewards are so nebulous, have a very clear cost.

Students who later learn they were targeted can suffer lasting psychological harm and life-long struggles with trust and self-censorship.[18] One Muslim student at Hunter College said that many fear that political engagement will result in being spied on.[19] Another CUNY student spoke of how she feels she doesn't know who to trust anymore.[20] At Brooklyn College, following revelations of NYPD surveillance on campus, attendance of Islam Awareness Week events plummeted.[21] One CUNY student withdrew from Muslim Student Association events after police came to his home to question him about his political opinions.[22] While the worst documented abuses may have ceased with the disbandment of the NYPD's "Demographics Unit," Many Muslim students still fear speaking in class about political issues, worried that they will be misinterpreted and investigated.[23]

---

[13] *Id.* at 15-18.

[14] *Id.* at 18.

[15] Chris Hawley, *NYPD Monitored Muslim Student All over Northeast*, ASSOCIATED PRESS, Feb 8. 2012, https://www.ap.org/ap-in-the-news/2012/nypd-monitored-muslim-students-all-over-northeast.

[16] N.Y. POLICE DEP'T, NYPD INTELLIGENCE DIVISION: STRATEGIC POSTURE 2006 17 (2006), https://www.nyclu.org/sites/default/files/releases/Handschu_Exhibit7b_%28StrategicPostureredacted%29_2.4.13.pdf.

[17] Goldman & Apuzzo, *supra* note 9.

[18] WATCHED (The Shorts Collective, LLC 2017).

[19] SHAMAS & ARASTU, *supra* note 7, at 23.

[20] *Id.* at 42.

[21] *Id.*

[22] *Id.* at 43.

(Cont'd on following page)

Younger students have not been immune to this. Some educators have sought Know-Your-Rights workshops to quell student fears of surveillance for children as young as eleven.[24]

These tragic accounts are not anomalous, they reflect an ongoing pattern of discriminatory police conduct. According to the Office of the Inspector General for the NYPD ("OIG"), over 95% of recent NYPD political and religious investigations targeted Muslim individuals and organizations.[25] The pattern of discriminatory surveillance is completely at odds with the fact that the overwhelming majority of terrorist attacks in the United States are committed by right-wing extremists and white supremacists. Let me repeat that fact, since it is so often lost in our media environment: right-wing extremists and white supremacists commit the overwhelming majority of terrorist attacks in the United States. That is not CAIR-NY's finding, that is the conclusion of groups ranging from the Anti-Defamation League, to the Southern Poverty Law Center, to the U.S. General Accountability Office.[26]

In contrast to the undercover practices documented above, the novel NYPD surveillance practices governed by the POST Act often are completely invisible to the target, making them much more dangerous to our freedom of speech and religion. The need for oversight is only heightened by the NYPD's clear track record of disregarding those few existing restrictions on surveillance of protected First Amendment activity. According to the OIG, over half of NYPD intelligence investigations continued even after the legal authorization for them expired.[27] Also, the OIG found that the NYPD frequently violated legal guidelines governing these investigations in other ways, such as through its use of boilerplate language in undercover officer authorization forms.[28]

(Cont'd from preceding page)

[23] *Id.* at 44-45.

[24] *Id.* at 43.

[25] OFFICE OF THE INSPECTOR GEN. FOR THE N.Y. POLICE DEP'T, N.Y. CITY DEP'T OF INVESTIGATION, AN INVESTIGATION OF NYPD'S COMPLIANCE WITH RULES GOVERNING INVESTIGATIONS OF POLITICAL ACTIVITY 1 n.1 (2016), https://www1.nyc.gov/assets/oignypd/downloads/pdf/oig_intel_report_823_final_for_release.pdf. In its investigation, the OIG reviewed a random selection of 20% of cases closed or discontinued between 2010 and 2015 of each case type. *Id.* at 14.

[26] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-17-300, COUNTERING VIOLENT EXTREMISM: ACTIONS NEEDED TO DEFINE STRATEGY AND ASSESS PROGRESS OF FEDERAL EFFORTS 4 (2017), https://www.gao.gov/assets/690/683984.pdf; David Neiwert, *Trump's Second Travel Ban Once Again Misidentifies Source of Domestic Terrorist Threat*, SOUTHERN POVERTY LAW CENTER (Mar. 13, 2017), https://www.splcenter.org/hatewatch/2017/03/13/trumps-second-travel-ban-once-again-misidentifies-source-domestic-terrorist-threat; *Murder and Extremism in the United States in 2016*, ANTI-DEFAMATION LEAGUE, https://www.adl.org/education/resources/reports/murder-and-extremism-in-the-united-states-in-2016 (last visited June 13, 2017).

[27] OFFICE OF THE INSPECTOR GEN. FOR THE N.Y. POLICE DEP'T, *supra* note 25, at 1.

(Cont'd on following page)

In light of the foregoing, we urge this City Council to enact the POST Act. This legislation will provide vital transparency for the NYPD's acquisition of, and use of, surveillance technology. I thank you for giving me the opportunity to address these urgent issues, and I look forward to working with the Council to safeguard the rights of Muslim New Yorkers in the months and years to come.

(Cont'd from preceding page)

[28] *Id.* Such conduct undermines the ability of independent bodies to effectively review police compliance with legal guidelines. *Id.* at 2.

131 West 33rd Street
Suite 601
New York, NY 10001
(212) 627-2227
www.thenyic.org

TESTIMONY OF THE NEW YORK IMMIGRATION COALITION
Int. 1482

Good Morning, thank you Public Safety Committee Chairperson Vanessa Gibson and Council Member Garodnick for allowing the New York Immigration Coalition (NYIC) to testify today on the POST Act (Int. 1482). My name is Muzna Ansari and I am the Immigration Policy Manager of the NYIC.

The NYIC is an umbrella policy and advocacy organization that represents over 150 non-profit members serving immigrants throughout New York State. For the last 30 years, the NYIC has engaged in advocacy at the city, state, and federal levels to protect immigrant communities. Due to the enforcement implications of surveillance and information sharing, the NYIC strongly supports passage of the Public Oversight of Surveillance Technology (POST) Act.

Thank you to the Council for introducing this important piece of legislation that will help ensure transparency and increase accountability of the NYPD. Given the Federal administration's unwavering attack on immigrant communities, it is vital now more than ever that the public be aware of what information the New York Police Department collects and subsequently shares with federal agencies. It is also critical in this political climate for the public to know *which* specific agencies this information is shared with.

Given the recent uptick in immigrant enforcement, immigrant communities are living in fear right now. In the eyes of undocumented immigrants, any interaction with local law enforcement can lead to significant ramifications. There are rampant rumors in the community of enforcement occurring as a result of interaction with various government agencies, particularly the NYPD. Immigrants are thus far less likely to trust law enforcement and far less likely to report crime or cooperate in the investigation and prosecution of criminal activity. Given the NYPD's history of surveillance of the Muslim community, there is also deep distrust amongst Muslim New Yorkers of local law enforcement.

At this critical time, it is vital that the public know what kinds of data the NYPD collects and disseminates, and with whom that information is shared. Currently, the NYPD faces no incentive or city requirement to withhold information from federal agencies, as surveillance technologies employed by the NYPD are often funded by federal grants or private donors. As a result, surveillance information sharing is currently inadequately monitored. Currently, New Yorkers do not know if, for example, the NYPD shares information gathered through surveillance with Immigration and Customs Enforcement (ICE).

While the City took a significant step in protecting immigrant communities by passing anti-detainer legislation, it must now apply that same level of commitment to ensure transparency regarding information sharing between the NYPD and federal agencies. We applaud the POST Act's requirement that the NYPD publicly share details regarding its use of surveillance technology and its dissemination of information collected. However, we call on the Council to take this bill one step further: the POST Act should explicitly require the NYPD to disclose *which agencies* it shares information with. This level of transparency and accountability will bring New York City closer to being a true "sanctuary city" and providing its immigrant communities the protection they deserve.

Thank you again to the Council for addressing this important issue and allowing the NYIC to testify. We look forward to working with you to ensure the privacy and rights of immigrants New Yorkers are upheld.

NYCLU
NEW YORK CIVIL LIBERTIES UNION

125 Broad Street, 19th floor
New York, NY 10004
212.607.3300
212.607.3318
www.nyclu.org

New York City Council Committee on Public Safety

Oversight Hearing on the POST Act (Int. 1482- 2017)

Testimony of the New York Civil Liberties Union

June 14, 2017

The New York Civil Liberties Union respectfully submits the following testimony in support of Int. 1482, the Public Oversight of Surveillance Technologies Act ("POST Act"). The NYCLU, the New York state affiliate of the American Civil Liberties Union, is a not-for-profit, non-partisan organization with eight offices across the state, and over 160,000 members and supporters statewide. The NYCLU's mission is to defend and promote the fundamental principles, rights and constitutional values embodied in the Bill of Rights of the U.S. Constitution and the Constitution of the State of New York, including the right to be free of unwarranted government surveillance and unjustified police actions.

The NYPD uses numerous forms of powerful, invasive and covert surveillance technologies to police New York City streets every day. These surveillance technologies can capture vast amounts of information about the places we visit, people we communicate with, the frequency of those communications, where we are located inside our home, and our most recent social media post. While surveillance technologies, by themselves, can pose significant risks to privacy, public health and other civil liberties and rights, the lack of transparency and oversight regarding how these technologies are acquired and used by the NYPD threatens our democracy. We urge the City Council to take action in defense of these principles by passing the POST Act into law.

To date, most of what we know regarding the NYPD's use of surveillance technologies is based on costly FOIL litigation by the NYCLU and other organizations, investigative journalism, and inquiries by the criminal defense community. Two examples that illustrate the problems created by the lack of transparency and oversight regarding the NYPD's acquisition and use of surveillance technologies are Stingrays and X-ray vans.

Stingrays are surveillance devices that mimic cell site towers and allow the NYPD to pinpoint a person's location, and some models can collect the phone numbers that a person has

been texting and calling as well as intercept the contents of communications. When Stingrays seek information for a targeted phone, they also sweep up information from hundreds or thousands of nearby cell phones. Stingray devices can cost over $100,000 per unit, and this does not include the additional costs of the training and maintenance packages that are necessary to use the devices.

In 2015, the NYCLU sent a FOIL request to the NYPD about Stingrays. We learned that the NYPD used these devices in more than 1,000 investigations since 2008, ranging from robbery and drug cases to criminal contempt of court. The NYPD has been successful in concealing their use of Stingrays because they are used without a warrant and without an internal policy guiding their use. Currently, all that the public knows regarding the NYPD's use of stingrays is based on the results of our FOIL request. We still do not know the full fiscal implications of the NYPD's use of Stingrays because they have failed to revealed how many they own or which models have been purchased. Stingrays raise a number of privacy and civil liberties concerns because they can track a person's location, including inside a home, a place of worship, or at a protest. It is also concerning that NYPD's failure to maintain adequate internal policies and safeguards for the data captured by Stingrays, can put many New Yorker's personal data at risk to malicious third party actors.

X-ray vans are military-grade surveillance equipment, which utilizes x-ray radiation to see inside of cars and buildings. These devices were used to search for roadside bombs in Afghanistan, but are also used on the streets of New York City. The company that manufacturers X-ray vans determined that the vans expose bystanders to a 40% larger dose of ionizing radiation than that delivered by similar airport scanners. Exposure to ionizing radiation can mutate DNA and increase the risk of cancer. In fact, the European Union and United States Transportation Security Administration banned the use of this type of radiation technology in airports citing privacy and health concerns. Additionally, X-ray vans costs between $729,000 and $825,000 per unit, which can have significant fiscal implications. Until ProPublica's FOIL lawsuit, nearly five years ago, which reveal some of what we know about x-ray vans, the NYPD has largely refused to disclose anything about how it uses x-ray vans on the streets of New York. The NYPD's attempt to keep these devices secret runs counter to best practices because other agencies, including the Department of Homeland Security, already revealed the same types of information sought by ProPublica in its FOIL lawsuit.

It is clear from these two examples that the NYPD's continued use of invasive surveillance technologies pose significant risks to privacy, public health, civil liberties and civil rights. The secretive and concealed process by which the NYPD obtains and uses these technologies runs counter to good governance principles, often violates the Constitution, and threatens the digital security of all New York City residents and visitors. The NYCLU has been at the forefront of bringing the NYPD's use of surveillance technology into the light for many

years. However, the public should not to have to learn about these technologies through costly litigation, and this is why we need the City Council to pass the POST Act now.

The POST Act will require the NYPD to publish impact and use policies for each surveillance technology it employs. These policies will include important information about each surveillance tool, including its description, capabilities, guidelines for use, security measures designed to protect any data it collects. The bill provides for audit mechanisms to ensure the NYPD is following its own policies. The POST Act will not inhibit the NYPD's ability to employ constitutionally sound investigatory and police practices to protect public safety, but it will ensure the NYPD is considering the potential risks and consequences of emerging and often invasive surveillance technologies.

The need for the City Council to pass the POST Act is all the more critical under the Trump Administration, who has fueled fears that the federal government will target certain communities for increased surveillance. It is also important for the City Council to know how municipal funds are being spent, particularly at a time the Trump Administration is threatening to cut or eliminate significant federal funding to New York City and State.

With the Trump Administration threatening to bully local law enforcement into carrying out its agenda, it is incumbent on the City Council to identify solutions for improving the relationship between police and communities. In addition to promoting broader transparency and oversight, the City Council must use its authority to reform the actual practices that create mistrust in the first place. It is time for the City Council to pass the Right to Know Act (Intro. 182-B and Intro. 541-A), two bills that have majority support among councilmembers and across the city. Along with the POST Act, the Right to Know Act will play a vital role in enhancing communication and trust between the NYPD and members of the public by promoting transparency and accountability in everyday police encounters. We urge the City Council to pass the POST Act and the Right to Know Act as soon as possible because the civil liberties and civil rights of New Yorkers depend on it.

FOR THE RECORD

NDS
HARLEM

TESTIMONY OF THE NEIGHBORHOOD DEFENDER SERVICE

before the

Committee on Public Safety

by

RICK JONES
Executive Director

June 14, 2017

WRITTEN TESTIMONY OF RICK JONES

INTRODUCTION

I am Rick Jones, Executive Director of the Neighborhood Defender Service (NDS), a community-based public defender office that provides high-quality legal services to residents of Northern Manhattan. NDS created a model for a neighborhood-based, comprehensive, client-centered approach to service that has led to improvement of defense services throughout New York State. Philanthropedia, the leading source of information about non-profit organizations, assembled a national panel of foundation professionals, academics, researchers, non-profit senior staff, policy makers and other professionals working in the field, to select and determine the best non-profits in the country and, through that process, NDS was named a top non-profit for 2011-2014.

In addition to being Executive Director of NDS, I have also taught on the faculty of Columbia Law School and the National Criminal Defense College (NCDC) for more than a decade. More importantly for present purposes, I am currently the President Elect of the National Association of Criminal Defense Lawyers (NACDL) and in July of this year in San Francisco will become the 59th President of NACDL. At NACDL I served on, and/or chaired, three national task forces that have led to groundbreaking reports which are relevant to this testimony. As a member, and/or chair, of the Task Forces on Problem-Solving Courts, Collateral Consequences and Body Cameras, I have had the opportunity to crisscross the country holding hearings and taking testimony from expert witnesses in the areas of criminal justice policy, reform and policing. I have also been a practicing attorney in New York City for nearly 30 years.

OVERSIGHT OF NYPD SURVEILLANCE TECHNOLOGY

In a July 2013 Department of Justice survey of police departments nationwide, 75 percent of respondents reported that they did not use body-worn cameras ("BWCs").[1] By 2015, a survey by the Major Cities Chiefs and Major County Sheriffs with the U.S. Department of Homeland Security found that 77 percent of respondents "intend to implement" or were otherwise testing the use of BWCs.[2] NYPD's own implementation of this surveillance technology—at the center of today's conversation—is thus in-line with a nationwide trend in law enforcement. Because of the size and prominence of the NYPD, however, the policies and procedures decided in this city are likely to influence departments around the country.

---

[1] Miller, Lindsay, Jessica Toliver, and Police Executive Research Forum. *Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned* (2014) Washington DC:OFFICE OF COMMUNITY POLICING SERVICES https://www.justice.gov/iso/opa/resources/472014912134715246869.pdf (last visited, June 12, 2017).
[2] Major Cities Chiefs and Major County Sheriffs, *Technology Needs- Body-Worn Cameras* (Dec. 2015). U.S. DEPARTMENT OF HOMELAND SECURITY'S OFFICE OF EMERGENCY COMMUNICATIONS https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/rvnT.EAJQwK4/v0 (last visited, June 12, 2017).

BWCs fit into a larger surveillance narrative in New York City. Military-grade technology has been deployed for years, yet not always with appropriate accompanying oversight. Between 2008 and 2015, for instance, Stingray devices were used over 1,000 times by the NYPD.[3] A technology capable of tracking cell phone location and activity can sweep up data of bystanders and has been deployed in New York City without the oversight of a warrant. Elsewhere, a lack of transparency in vast data-gathering efforts at facial recognition have resulted in private groups suing the Department to release information about a program that many claim lacks sufficient oversight.[4]

Within this climate, the current test of BWCs and efforts to guide data collection and dissemination with policies such as the one discussed today are welcome developments. Nevertheless, a comparative study and codified oversight may be insufficient to overcome numerous well-documented limitations in surveillance technologies. While my remarks will focus on BWC, many of the concerns I will touch upon apply to other devices as well.

BODY-WORN CAMERAS

The NYPD's pilot program for BWCs began a little over a month ago. It pairs 1,200 officers with devices across 20 precincts and then seeks to compare factors such as officer performance, civilian complaints, crime statistics, and judicial outcomes with 20 similarly situated precincts without the devices.[5] At best, BWCs improve police conduct in interactions with civilians and foster trust with the public for an initial, finite period of time. Unfortunately, however, studies are beginning to show that even these threshold ideals are often unmet. The problems explained below highlight the dangers of a community relying upon a technology that can be manipulated, subjective and unrepresentative of police interactions.

a) BWCS DO NOT FOSTER POLICE TRANSPARENCY AND ACCOUNTABILITY

There are poor records of police compliance with BWCs. An independent monitor investigating the New Orleans Police Department's use of BWCs in 2010 expressed suspicion regarding how frequently BWCs malfunctioned and failed to record during crucial moments.[6] They reviewed 145 use of force reports, and found footage for only 49 incidents. A Phoenix study found that

---

[3] American Civil Liberties Union, *NYPD Has Used Stingrays More Than 1,000 Times Since 2008* (Feb. 2016) NYACLU https://www.nyclu.org/en/press-releases/nypd-has-used-stingrays-more-1000-times-2008 (last visited, June 12, 2017).

[4] Dustin Volz, *Privacy Group Sues NYPD for Release of Facial-Recognition Documents* (May 2017) Washington DC, *REUTERS* http://www.reuters.com/article/us-usa-cyber-face-recognition-idUSKBN17Y1Z1 (last visited, June 12, 2017).

[5] Ashley Southall, *Do Body Cameras Help Policing? 1,200 New York Officers Aim to Find Out* (April 2017) New York: THE NEW YORK TIMES https://www.nytimes.com/2017/04/26/nyregion/do-body-cameras-help-policing-1200-new-york-officers-aim-to-find-out.html?mcubz=0 (last visited, June 12, 2017).

[6] Alexandra Mateescu, Alex Rosenblat & Danah Boyd, *Police Body-Worn Cameras*, DATA & SOCIETY RESEARCH INSTITUTE, (Feb. 2015).

officer compliance with a mandatory recording policy started at 40 percent, and by the end of the trial period had dropped to 13 percent; only about 20 percent of the total of the interactions that were supposed to be recorded actually were.[7] **Not surprising, studies suggest that the use of BWCs do not build trust with citizens.[8]**

Dash camera footage under police control has faced similar issues with law enforcement's reluctance to be transparent and comply with its policies. With dash cams, officers undermined the technology: a 2002 study found that 23 percent of the time that officers were turning in the VHS tape with their footage, they were running it through a scrambling machine to destroy it.[9] About 95 percent of the time, officers were not using the audio recording feature. Other issues include:

- For over a year, the police department in Chicago fought the release of dash camera footage of the police killing of 17-year-old Laquan MacDonald.[10]
- The BWCs of the officers who killed Alton Sterling in Baton Rouge were dislodged during the altercation, resulting in very poor-quality video and thus showcasing the limitations of such recordings.[11]

Manipulation continues to be a consistent problem. In October of 2015, the Washington Post reported that less than half of footage of police shootings resulting in fatalities was released to the public and much of the footage released was edited.[12] In July 2016, North Carolina Gov. Pat McCrory signed new legislation that prevents the public from accessing footage from law enforcement BWCs and dashboard cameras.[13] Under this law, only a person whose image or voice is captured on a recording can request to view it. Only a look at the video is allowed; to receive a copy of the footage, a petition must be made to the court to order its release.[14] Groups like Black Youth Project 100, Black Lives Matter, Million Hoodies, the Advancement Project and any number of criminal justice groups, both in DC and across the country, oppose the wanton use of policy body worn cameras: "More cameras means exactly what it says: more

---

[7] Seth Stoughton, Assistant Professor of Law at the University of South Carolina School of Law, Task Force Witness Testimony.
[8] Ellen Meyers, *Arlington Police Chief: Body Cameras Aren't Effective In Building Trust with the Public*, (July 2016) THE DALLAS MORNING NEWS, http://www.dallasnews.com/news/crime/headlines/20160711-arlington-police-chief-body-cameras-aren-t-effective-in-building-trust-with-public.ece (last visited, June 12, 2017).
[9] Stoughton, *supra* note 3.
[10] *New York State Assembly Standing Committees On Codes, The Judiciary, and Governmental Operations,* (Dec. 8, 2015) (statement of Alice L. Fontier, Vice President, New York State Association of Criminal Defense Lawyers).
[11] Bryn Stole, *Baton Rouge Police Shooting Raises Questions About Officer-Worn Cameras* (July 2016). REUTERS, http://www.reuters.com/article/us-louisiana-police-body-cameras-idUSKCN0ZM2MO (last visited, June 12, 2017).
[12] *New York State Assembly Standing Committees On Codes, The Judiciary, and Governmental Operations,* (Dec. 8, 2015) (statement of Center for Constitutional Rights).
[13] Emanuella Grinberg, *North Carolina Law Blocks Release of Police Recording* (July 2016) .CNN. http://www.cnn.com/2016/07/12/politics/north-carolina-police-recording-law/ (last visited, June 12, 2017).
[14] Id.

cameras. It does not necessarily mean more accountability. What it definitely means is more cameras."[15]

b) BWC FOOTAGE DOES NOT PROVIDE AN ACCURATE REPRESENTATION OF POLICE-CITIZEN ENCOUNTERS

There is a human tendency to think that camera footage presents an objective, neutral record of events, which is not accurate. BWCs are fixed to one part of the officer's body, usually the chest, and thus provide a skewed perspective onto the situation. From this vantage point, several inches lower than the officer's sightline, an individual may appear larger and more menacing than he is in reality. There is an implicit camera perspective bias, a tendency to view the video in a way that favors the perspective we are sharing.[16]

Additional limitations are inherent in BWCs because the footage does not show off-camera events, like the officer's body language. The footage does not capture other senses, like smell, and can be misleading.[17] Narration and pre-conceived notions of law enforcement and threat levels can often lead to misleading interpretations of footage.[18] Cognitive bias intrudes on videos similar to how it guides our interpretation of day-to-day life.[19] Once a suggestion has been implanted in our brains, we may discount or disagree with it, but we cannot undo it.[20] Police have learned to narrate citizen encounters in real time such that the soundtrack accompanying the video serves more to distort, rather than underscore, the reality of the interaction. When viewed from a distance by an objective camera that captures the entire scene, body camera video accompanied by police narratives bears no rational relation to events as they actually occurred.

c) BWC RECORDING CAN BE USED FOR MASS SURVEILLANCE AND BIOMETRIC DATA COLLECTION, FURTHER VICTIMIZING OVER-POLICED COMMUNITIES

---

[15] Malkia Cyril, Executive Director of the Center for Media Justice, Leader, Black Lives Movement Network, Task Force Witness Testimony.
[16] Stoughton, *supra* note 7.
[17] Id.
[18] Timothy Williams, James Thomas, Samuel Jacoby and Damien Cave, *Police Body Cameras: What Do You See?* (April 2016) THE NEW YORK TIMES. https://www.nytimes.com/interactive/2016/04/01/us/police-bodycam-video.html?mcubz=0. (last visited, June 12, 2017).
[19] Id.
[20] Janet Vertesi, *The Problem With Police Body Cameras* (May 2015). TIME, http://time.com/3843157/the-problem-with-police-body-cameras/ (last visited, June 13, 2017).

Biometric identifiers currently in use include fingerprints, palm veins, facial recognition, DNA, palm print, hand geometry, iris recognition, retina, odor/scent and voice. Facial recognition technologies greatly threaten civilian privacy and can be used to read thousands of faces, create mathematical representations of those faces and cross check that information against mug shots, employment records and background check databases.[21] Federal privacy laws currently do not offer protection from government biometric data collection.[22]

Michelle Alexander, author of *The New Jim Crow*, believes that body cameras are not a solution, pointing out that their technology could be used to further other agendas, like monitoring communities of color.[23] In addition to prosecution, increased surveillance can be used for evidence collection and impermissible review of footage in search of any uncharged crimes: **"What is the history of additional watching in communities of color and those who are most likely to be impacted and observed by this? Watching generally means criminalization. It does not help, it hurts."[24]**

Issues in how BWC data is collected, stored, analyzed and owned fit within broader concerns about predictive policing.[25] A recent report by Taser (now "Axon")—a leading manufacturer of BWC devices—noted the dangers of biometric and pattern recognition in the not-too-distant future:

> [T]he fact that I could potentially walk down the street with a camera in real time, scanning faces, doing facial recognition while it's recording, sending that data to the cloud for real-time analysis, have that data come back and somebody tell me, "That guy in the red hat, red shoes you just passed, he's wanted for burglary" That type of real-time, big data analysis application would be huge.[26]

Huge- and likely wrong. More than 50 percent of the criminal histories held by the FBI, the largest repository of criminal history information, are wrong.[27] The percentages are even higher when we look into state, county and municipal databases. The marriage of facial recognition

---

[21] Samantha Lee, *Open Face: Striking the Balance Between Privacy and Security with the FBI's Next Generation Identification System,* J. LEGIS. 264, (2014-2015).
[22] Id.
[23] Michelle Alexander and Erin Loeb, *Michelle Alexander on Racial Justice, Mass Incarceration and Black Lives Matter* (Jan. 2016). FORD FOUNDATION, http://www.fordfoundation.org/ideas/equals-change-blog/posts/michelle-alexander-on-racial-justice-mass-incarceration-and-black-lives-matter/ (last visited, June 12, 2017).
[24] Cyril, *supra* note 15.
[25] Martin Kaste, *Should the Police Control Their Own Body Camera Footage?* (May 2017) NPR. http://www.npr.org/2017/05/25/529905669/should-the-police-control-their-own-body-camera-footage (last visited, June 12, 2017).
[26] Taser, *Law Enforcement Technology Report* (2017) https://assets.documentcloud.org/documents/3679537/Taser-2017-Law-Enforcement-Technology-Report.pdf (last visited, June 12, 2017).
[27] Madeline Neighly, *The Faulty FBI Files That Can Ruin Your Life* (Sept. 2013). CNN, http://www.cnn.com/2013/09/02/opinion/neighly-fbi-background-checks/index.html (last visited, June 13, 2017).

technology and predictive policing leads to the unlawful stop, search, arrest and charging of untold numbers of American citizens, many falsely accused, most people of color and poor.

Algorithmic and data-driven decision-making in the criminal justice system is already fraught with questions of Constitutional rights. The introduction of BWC technology adds privacy and a layer of ubiquitous surveillance to the debate. "Offender-based modelling" marshals factors such as age, personal history, associations, and location to guide decisions like incarceration and social services.[28] BWCs have the potential to transfer that model to any sidewalk and street corner a police department may choose, with untold consequences on the effects such surveillance would have on a community.

d) TO THE EXTENT THAT BWCS ARE BEING EMPLOYED, THE FOLLOWING GUIDELINES WILL MINIMIZE ABUSE AND MISUSE

- **BWCs must be head-mounted**
  Although in the U.S. most cameras are either chest or lapel mounted, some countries place them on hats or helmets.[29] This provides a more precise depiction of events, since the perspective is a more accurate portrayal of the officer's view point and there is less distortion of individual's height and behavior.

- **Only BWCs with a wide field of view should be used**
  Some cameras are being specifically marketed to law enforcement because of their narrow field of view, which could be decreased from 165 degrees to as little as 50 or 60 degrees.[30] Wide-angle lenses, however, provides the most accurate perspective of events in their entirety as they unfold.

- **BWCs must not contain any biometric data collection technologies**
  There is no need for such capabilities given the stated purpose of BWCs. Biometric data collection leads to over-surveillance of already over-policed communities, exacerbating existing issues in law enforcement relations with low-income communities.[31] These technologies threaten civilian privacy and undermine the purpose of BWCs.

---

[28] Aaron Shapiro, *Reform Predictive Policing* (Jan. 2017) NATURE. http://www.nature.com/news/reform-predictive-policing-1.21338 (last visited, June 12, 2017).
[29] Stoughton, *supra* note 3.
[30] Aliya Rahman, Former Code for Progress Director, Task Force Witness Testimony.
[31] Scott Simpson, *Civil Rights, Privacy, and Media Rights Groups Release Principles for Law Enforcement Body Worn Cameras,* THE LEADERSHIP CONFERENCE, May 15, 2015; *Considering Police Body Cameras,* 128 HARV. L. REV. 1794, (Apr. 10, 2015); *New York State Assembly Standing Committees On Codes, The Judiciary, and Governmental Operations,* (Dec. 8, 2015) (statement of Veronica Bayetti Flores, Steering Community Member, Communities United for Police Reform).

- **BWCs must have a visible light that turns on when the camera is recording**
  This will provide notice to the public that they are being recorded.[32]

- **BWCs must be controlled and monitored remotely by a third, independent, party**
  An Independent Monitoring Board (IMB) should be appointed to control access to all body camera footage: one board member appointed by the Mayor, one by law enforcement, one by the City Council, one by the Criminal Defense Bar and one by community groups. The IMB would hire staff to implement the policies set forth by the board. The IMB policies would control when the camera is turned off or muted, should there be an officer or civilian request.

- **The footage must be retained until the statute of limitations for a civilian complaint for officer misconduct expires**
  If there is an arrest, footage must be stored for 2 years. In capital punishment cases, footage must be retained until all appeals have been exhausted. Defense counsel must be permitted to flag any footage believed to be relevant to any prosecution, such as footage indicating a pattern of behavior or supportive of an alibi.

- **Video footage must be stored in a cloud-based storage system**
  It should be encrypted to ensure no outside party can have access. There must be safeguards in place against data manipulation, like digital fingerprints.

- **All parties, including law enforcement, must be granted access to body camera footage at the same time**
  No one outside the IMB should have access to any of the video footage unless it is necessary for a civil or criminal proceeding, citizen complaint or for investigative purposes pursuant to Law Enforcement Misconduct Statute 42 U.S.C. §14141. In criminal proceedings, both the prosecution and defense should have the ability to subpoena the footage and each side should be granted access to the footage at the same time. In civil proceedings, both parties should have the ability to subpoena the footage and each side should be granted access to the footage at the same time. In citizen complaint, citizens that are the subject of the footage should have clear rights dictating how to acquire access to the footage and the footage will be made available in a timely manner. In a §14141 cause of action, a federal judge or magistrate must determine whether the Department of Justice (DOJ) will be granted access to BWC footage and whether redactions are needed for the purpose of identifying a pattern and practice of misconduct.

---

[32] Mitch Mitchell, *Tarrant County Police Race to Join Body Camera Bandwagon* (Oct. 23, 2015). STAR TELEGRAM. http://www.star-telegram.com/news/local/community/fort-worth/article41250195.html (last visited, June 12, 2017).

e) THE BETTER PRACTICE FOR ENSURING POLICE ACCOUNTABILITY AND TRANSPARENCY IS TO ENCOURAGE, SUPPORT, AND INSTITUTIONALIZE CITIZEN FILMING OF POLICE-CITIZEN ENCOUNTERS

Rather than facilitating a surveillance state, **placing the video in the hands of the citizen shifts the balance of power and obviates major police issues such as BWC misuse, subjective viewer bias and mass surveillance.** Civilian control over the recording device transfers the decision of when to switch the BWC 'on' away from the individual officer, and puts it in the hands of local observers.[33] This policy has the potential to avoid police officers' frequent claims of BWC failure during police-citizen encounters.

Additionally, citizen filming removes police departments from their role as gatekeepers of video footage, dismantling "the traditional monopoly that police departments possess over the evidence of, and narratives structuring, their behavior on the street."[34] Footage recorded by citizens can provide neutral, objective, wide-angle representation of the scene, eliminating the bias inherent in the subjective perspective provided by police BWCs. By placing control of the footage in the hands of citizens, the threat of the use of BWC footage as a tool of state mass surveillance of over-policed communities is eliminated.

Scholars have shown that **including citizens in the policing process promotes legitimacy and improves police-community relations.**[35] Civilian videos allow individuals to challenge official accounts of police shootings and have a voice in the public narrative, thus keeping law enforcement accountable.[36] The power shift inherent in the change of the locus of control over camera footage "promotes democratic engagement so that other forms of accountability – legislative, executive and administrative, both federal and local – can more accurately represent the people to whom they are supposed to be accountable."[37] In 2015, the NYPD's Civilian Complaint Review Board found that more claims of excessive force are being investigated and substantiated as a result of corroborating civilian video evidence.[38]

The phenomenon of organized 'copwatching', whereby groups of citizens carry visible recording devices and film police-citizen interactions, is on the rise.[39] **Sociologists have termed this filming of authority figures by disempowered populations "*sous*veillance."[40] It represents a more effective deterrent of police misconduct because the cameras and the footage remain**

---

[33] Jocelyn Simonson, *Beyond Body Cameras: Defending a Robust Right to Record the Police,* 104 GEO. L. REV. (forthcoming 2016) (manuscript at 10).
[34] Id. at 11.
[35] Michael D. Reisig, Community and Problem-Oriented Policing, 39 CRIME & JUST. 1, 2–40 (2010).
[36] Rebecca McCray, *As More Videos Surface, Citizens Remind Police of Their Right to Film* (July 2016). TAKEPART, http://www.takepart.com/article/2016/07/09/filming-nypd (last visited, June 12, 2017).
[37] Jocelyn Simonson, *Copwatching*, CALIF. L. REV. 391, 435 (2016).
[38] Tess Owen, *People are Filming the NYPD – And It's Making it Easier to Investigate Misconduct* (Sept. 2015).VICE NEWS, https://news.vice.com/article/people-are-filming-the-nypd-and-its-making-it-easier-to-investigate-misconduct (last visited, June 12, 2017).
[39] Jocelyn Simonson, *Copwatching*, CALIF. L. REV. 391, 394 (2016).
[40] Steve Mann & Joseph Ferenbok, *New Media and the Power Politics of Sousveillance in a Surveillance-Dominated World*, 11 SURVEILLANCE & SOC'Y 18, 26 (2013).

out of the control of law enforcement, and in the hands of civilians.[41] There are several popular mobile applications available on the market, like CopWatch and Mobile Justice, which help people record videos of police-citizen encounters and upload them directly onto the Internet.[42]

Footage from citizens provides a more complete account of events as they actually transpired and allows traditionally powerless populations to have a direct input into policing decisions.[43] Citizen filming gives poor communities the ability to share their experiences with law enforcement with more privileged individuals, whose daily interactions with the police may differ significantly.[44] It increases awareness of police misconduct among a wider part of the population and provides a point of view of communities whose voice is usually left out of debates about policing practices.[45]

Despite this promising trend in citizen involvement, police departments have not been supportive of citizen filming. **The right to film police-citizen encounters has been firmly established in law.**[46] According to Jay Stanley of the ACLU, **however, "there is a widespread, continuing pattern of law enforcement ordering people to stop taking photographs or video in public places and arresting those who fail to comply."**[47] In New York City, government and law enforcement "maintain a widespread practice and custom of permitting NYPD officers to interfere with the First Amendment rights of individuals who, without interfering with police activity, record or attempt to record such activity in public places."[48] In Boston, the Police Commissioner asked the legislature to regulate citizen filming by criminalizing the act of recording when it is done close to the officers.[49]

CONCLUSION

Despite commonly being portrayed as a "cure-all" in law enforcement—from the standpoint of community relations and police misconduct—BWC technology raises far more concerns than it addresses. When developed, BWCs were introduced as a means to shift power in police interactions to citizens by providing a true account of confrontations and a check on law

---

[41] Simonson, *supra* note 26, at 414.
[42] Amanda Hess, *Justice Through a Len* (April 2015). SLATE, http://www.slate.com/articles/technology/users/2015/04/copwatch_mobile_justice_and_other_apps_for_citizens_filming_police_encounters.html (last visited, June 12, 2017).
[42] Complaint & Demand for Jury Trial at 8, An v. City of N.Y. (July 6, 2016).
[43] Id.
[44] Simonson, *supra* note 26, at 419.
[45] Id. at 435.
[46] Stipulation & Order at 1, Black v. Codd, 73 Civ. 5283 (June 1st, 1977).
[47] Sam Adler-Bell, *That's What You Get for Filming the Police* (May 2015). TRUTHOUT, http://www.truth-out.org/news/item/30628-that-s-what-you-get-for-filming-the-police (last visited, June 12, 2017).
[48] Complaint & Demand for Jury Trial at 8, An v. City of N.Y. (July 6, 2016).
[49] Matt Stout, *Boston Police Commissioner Wants Law to Push Back on Camera-Toting Cop Watchers* (Aug. 2015). BOSTON HERALD, http://www.bostonherald.com/news_opinion/local_coverage/2015/08/boston_police_commissioner_wants_law_to_push_back_on_camera (last visited, June 12, 2017).

enforcement behavior. Over time, and unsurprisingly, studies suggest that the actual balance of power from BWCs has swung toward the police.[50]

The physical limitations of vantage-points, angles and footage obscured by movement often create a representation that is far from a complete depiction of an event as it occurred. Less-innocuous trends in failure rates, editing and misleading police narration suggest that the misconduct that BWCs promised to address is just being transferred to the operation and manipulation of the devices themselves.

Finally, surveillance and recognition data from BWCs present troubling potential for the over-policed, the disadvantaged and communities of color. Rather than the goal of improving police/community rapport, ubiquitous surveillance creates a dynamic of antagonism and distrust. New York City should carefully weigh the long-term studies into the impact of BWCs and resist becoming a nationwide advocate for their adoption.

[50] Robinson Meyer, *Body Cameras are Betraying Their Promise* (Sept 2016). THE ATLANTIC. https://www.theatlantic.com/technology/archive/2016/09/body-cameras-are-just-making-police-departments-more-powerful/502421/ (last visited, June 12, 2017).

New York City Council Committee on Public Safety

Hearing on the POST Act (Int. 1482-2017)

Testimony of Center for Democracy & Technology, Campaign Zero, South Asian Americans Leading Together (SAALT), Tenth Amendment Center, Restore the Fourth, Defending Rights and Dissent, Open Technology Institute, Electronic Frontier Foundation, National Network of Arab American Communities, Council of American-Islamic Relations (CAIR National), Fight for the Future, Crypto Harlem, Access Now, Million Hoodies Movement for Justice, American Civil Liberties Union (ACLU)

June 14, 2017

The Center for Democracy & Technology, Campaign Zero, South Asian Americans Leading Together (SAALT), Tenth Amendment Center, Restore the Fourth, Defending Rights and Dissent, Open Technology Institute, Electronic Frontier Foundation, National Network of Arab American Communities, Council of American-Islamic Relations (CAIR National), Fight for the Future, Crypto Harlem, Access Now, Million Hoodies Movement for Justice, and American Civil Liberties Union (ACLU) respectfully submit the following testimony in support of Int. 1482, the Public Oversight of Surveillance Technologies Act ("POST Act"). We thank the Public Safety Committee for holding a hearing on this important legislation, especially at a time when the federal government is actively dismantling the right to privacy. The aforementioned groups urge the City Council pass the POST Act.

The increasing use of surveillance technologies by local police in cities across America, especially against communities of color and other unjustly targeted and politically unpopular groups, is creating oppressive and stigmatizing environments in which every community member is treated like a prospective criminal. Many communities of color and low-income communities have been turned into virtual prisons where their residents' public behavior is monitored and scrutinized 24 hours a day. Yet, despite this perpetual surveillance, there is very little evidence that these technologies reduce crime or prevent terrorism.[1]

Almost every week we learn of new surveillance technologies that are being used by law enforcement agencies around the country. These revelations are often a result of investigative reporting or lawsuits. In most cities, decisions to acquire and use surveillance technologies are made in secret by police departments without any knowledge or input from the public or their

[1] Bruce Schneier, *Focus on the Threat*, N.Y. Times, Room for Debate, Mar. 3, 2010, https://roomfordebate.blogs.nytimes.com/2010/05/03/times-square-bombs-and-big-crowds/?src=tptw#bruce; Michael S. Schmidt, *F.B.I. Said to Find It Could Not Have Averted Boston Attack*, N.Y. Times, Aug. 1, 2013, http://www.nytimes.com/2013/08/02/us/fbi-said-to-conclude-it-could-not-have-averted-boston-attack.html?partner=rss&emc=rss&smid=tw-thecaucus&_r=3&.

elected officials. This has to stop. The New York City Council should be empowered to provide greater transparency and oversight over the NYPD's acquisition and use of surveillance technologies.

When used indiscriminately, surveillance technologies create oppressive, stigmatizing environments, especially for communities that are disproportionately targeted by their use, such as communities of color, low income communities, and politically active communities. Rather than allowing the police to unilaterally decide if and how surveillance technologies may be acquired and used, we believe local communities and their elected officials should be informed in order to provide greater input and oversight.

Procedures for promoting greater transparency and oversight are necessary because it is clear that without such procedures, law enforcement use of surveillance technologies will often fail to adopt appropriate limitations and adhere to best practices. For instance, a New York Civil Liberties Union FOIL request revealed that the NYPD used Stingrays, a surveillance device that allow authorities to spy on cell phones in the area by mimicking a cell tower, over 1,000 times since 2008.[2] The NYPD also disclosed that it has no written policy for use of the Stingrays, and follows a practice of obtaining only lower-level court orders rather than warrants.[3] The process for considering the use of surveillance technologies should be transparent and well-informed. Transparency helps facilitate public debate that will benefit the NYPD's development of policies that reflect best practices, do not inhibit their investigatory powers, and protect the civil rights and civil liberties of New Yorkers.

We thank the New York City Council's Public Safety Committee for bringing attention to this important issue. We urge the City Council to pass Int. 1482, and hope that the City Council will continue to take an active role in preserving New Yorkers' civil rights and liberties and protecting their privacy.

[2] Press Release, New York Civil Liberties Union, NYPD HAS USED STINGRAYS MORE THAN 1,000 TIMES SINCE 2008 (Feb. 11, 2016), https://www.nyclu.org/en/press-releases/nypd-has-used-stingrays-more-1000-times-2008.
[3] *Id.*

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1482 Res. No. _____

☒ in favor ☐ in opposition

Date: 6-14-17

(PLEASE PRINT)

Name: Harlan Yu

Address: 1323 QUINCY ST. NW, WASHINGTON, DC 20011

I represent: UPTURN

Address: 1015 15TH ST. NW SUITE 600, WASHINGTON DC 20005

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1482 Res. No. _____

☑ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Yung-mi Lee

Address: _____

I represent: Brooklyn Defender Services

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1482 Res. No. _____

☑ in favor ☐ in opposition

Date: 6/14/17

(PLEASE PRINT)

Name: Wesley Alexis

Address: _____

I represent: Supporters of #1482 Privacy

Address: _____

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1482 Res. No. _____

☒ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: THEO CHINO

Address: 640 48D

I represent: Resbee the Earth

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1482 Res. No. _____

☐ in favor ☒ in opposition

Date: 6/14/17

(PLEASE PRINT)

Name: Deputy Commissioner Legal Matters / Lawrence Byrne

Address: _____

I represent: NYPD

Address: 1 Police Plaza

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1482 Res. No. _____

☒ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Michael Price

Address: 120 Broadway, New York

I represent: Bronx Defenders

Address: _____

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Kelly Gracia Pha

Address: 534 W 187th #7N NY

I represent: Jails Action Coalition

Address: 40 Rector St.

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1482 Res. No. _____

☑ in favor ☐ in opposition

Date: 6/14/17

(PLEASE PRINT)

Name: MUZNA ANSARI

Address: 131 W. 33rd Street, New York NY 10001

I represent: New York Immigration Coalition

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1482 Res. No. _____

☑ in favor ☐ in opposition

Date: 6/14/17

(PLEASE PRINT)

Name: CHAD MARLOW

Address: 125 BROAD ST., NY, NY

I represent: ACLU

Address: _____

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1482 Res. No. _____

☑ in favor ☐ in opposition

Date: 6/14/17

(PLEASE PRINT)

Name: Rashida Richardson

Address: _____

I represent: New York Civil Liberties Union

Address: 125 Broad Street

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☑ in favor ☐ in opposition

Date: 6/14

(PLEASE PRINT)

Name: Tovaki Komatsu

Address: One Penn Plaza

I represent: Self

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1482 Res. No. _____

☑ in favor ☐ in opposition

Date: 6/14/17

(PLEASE PRINT)

Name: Jerome Greco

Address: 49 Thomas Street, New York, NY 10013

I represent: The Legal Aid Society

Address: 199 Water Street, New York, NY

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1482 Res. No. ~~#R~~

☒ in favor ☐ in opposition

Date: 6/14/17

(PLEASE PRINT)

Name: Albert Cahn

Address:

I represent: CAIR-NY

Address: 46-01 20th Ave, Queens, NY 11105

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1482 Res. No. ~~#R~~

☐ in favor ☒ in opposition

Date: 6/14/17

(PLEASE PRINT)

Name: Director Oleg Chernyavsky

Address: 1 Police Plaza

I represent: NYPD

Address:

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1482 Res. No. _____

☐ in favor ☒ in opposition

Date: 6/14/17

(PLEASE PRINT)

Name: Chief Robert Boyce - NYPD Chief of Detectives

Address: 1PP

I represent: NYPD

Address: _____

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1482 Res. No. _____

☐ in favor ☒ in opposition

Date: 6/14/17

NYPD **(PLEASE PRINT)**

Name: John Miller - Deputy Commissioner, Intelligence & Counterterrorism

Address: 1PP

I represent: NYPD

Address: NYPD

Please complete this card and return to the Sergeant-at-Arms