

NYC COUNCIL
CITY OF NEW YORK

----- X

TRANSCRIPT OF THE MINUTES

Of the

COMMITTEE ON PUBLIC SAFETY

----- X

June 14, 2017
Start: 10:20 a.m.
Recess: 1:22 p.m.

HELD AT: Council Chambers - City Hall

B E F O R E: VANESSA L. GIBSON
Chairperson

COUNCIL MEMBERS: Vincent J. Gentile
James Vacca
Julissa Ferreras-Copeland
Jumaane D. Williams
Robert E. Cornegy, Jr.
Chaim M. Deutsch
Rafael Espinal, Jr.
Rory I. Lancman
Ritchie J. Torres,
Steven Matteo

A P P E A R A N C E S (CONTINUED)

Oleg Chernyavsky, Director
Legislative Affairs
New York City Police Department

Larry Byrne, Deputy Commissioner
Legal Affairs
New York City Police Department

John Miller, Deputy Commissioner
Intelligence and Counter-Terrorism

Robert Boyce, Chief of Detectives
New York City Police Department

Chad Marlow, Attorney
American Civil Liberties Union ACLU

Rashida Richardson, Legislative Counsel
New York Civil Liberties Union

Albert Kahn, Legal Director
Care New York

Michael Price, Counsel
Liberty & National Security Program
Brennan Center for Justice

Muzna Ansari, Immigration Policy Manager
New York Immigration Coalition, NYIC

Wesley Alexis, Supporter
NYC Privacy Board Advocates

Jerome Greco, Staff Attorney
Digital Forensic Unit
Legal Aid Society

C.O. Chin
Restore the Fourth

Kelly Grace-Price

Yung-Mi Lee, Supervising Criminal Defense Attorney
Brooklyn Defender Services

Towaki Komatsu, U.S. Navy veteran

Harlan Yu, Upturn

2 [sound check, pause] [gavel]

3 SERGEANT-AT-ARMS: Quiet, please.

4 CHAIRPERSON GIBSON: Good morning, ladies
5 and gentlemen. Welcome to the City Council Chambers.
6 I am Council Member Vanessa Gibson of District 16 in
7 the Bronx and I'm proud to serve as Chair of the
8 Committee on Public Safety. I welcome each and every
9 one of you here to our hearing this morning, and
10 before I begin, I certainly on behalf of my
11 colleagues and I want to express our thoughts and
12 prayers of recovery and healing to the House Majority
13 Congress Member Steve Scalise and law enforcement and
14 others that were injured this morning in a horrific
15 shooting that took place in Alexandria, Virginia. We
16 want to pray for everyone's survival and recovery,
17 and also we want to continue to keep in our thoughts
18 and prayers the recovery of NYPD Officer Dalsh Veve
19 of the 67th Precinct in Brooklyn and also I'm asking
20 you on behalf of my district in the Bronx to continue
21 to pray for the healing and strength of five-year-old
22 Jaheem Hunter who was unfortunately shot on his
23 birthday last Monday. On behalf of the family who
24 are friends of mine, I ask you to keep them in your

2 prayers, and certainly pray for Police Officer Veve.
3 Thank you very much.

4 This morning we are hearing legislation
5 Intro 1482, the public oversight of Surveillance
6 Technology Act or called the POST Act. This is
7 legislation, which I am proud to co-sponsor with
8 Council Member Dan Garodnick will bring transparency
9 to the Police Department's use of technology, a
10 necessary step in our overall goal of continuing to
11 improve our police and community relations all while
12 keeping every New Yorker safe. Under the POST Act
13 the NYPD would be required to publish a policy for
14 the impact and the use of surveillance technologies
15 in particular outlining the capabilities, the rules,
16 processes, guidelines, training requirements and
17 safeguards that are used to protect data collected by
18 the department. The public would have an opportunity
19 to review and comment on the department's policy
20 regarding the use of surveillance technologies and
21 submit such comments to the department for
22 consideration. The final policy would be submitted
23 to the City Council and the Mayor as well as posted
24 on the department's website. With the expansion of
25 technology capabilities across the country, the NYPD

2 has naturally increased its use of various
3 surveillance technologies over the last several
4 years. Such technologies range from ShotSpotter, the
5 Gunshot Detection and Locator mechanism, and License
6 Plate Readers to military grade x-ray vans that can
7 look into buildings and vehicles as well as Cell-Site
8 Simulators. While the NYPD has shared information
9 with this Council on the use of some of this
10 technology and equipment, at the local level there is
11 no formal oversight or legislative input on the use
12 or the acquisition of these potentially invasive
13 technologies. According to the department between
14 2008 and 2015, the NYPD used Cell-Site Stimulators, a
15 device that mimics a cell tower and allows the police
16 to pinpoint a person's actual location 1,016 times.
17 This technology and others that are used by the
18 department have the capability to collect and store
19 data from everyday New Yorkers as well as those
20 suspected of committing crimes, and for that reason,
21 we believe that there should be an opportunity to
22 weigh in on that use. We are aware that the
23 department has serious concerns regarding today's
24 legislation. They believe that disclosure of
25 surveillance technology is counter to the city's best

2 interest in public safety. It is indeed a concern
3 that by making certain technologies public, those
4 looking to harm us maybe able to develop methods to
5 evade detection from the surveillance equipment. We
6 absolutely are not looking to restrict any ability by
7 the NYPD to fight crime nor protect this city.
8 However, every New Yorker should have-should not have
9 to choose between safety and privacy. Improving the
10 community's ability to trust, communicate and work
11 together with our law enforcements is always
12 important to our collective goal of keeping New
13 Yorkers safe. I believe there is a path that
14 balances both the civil liberties of our residents
15 with the safety of this city. In fact, other cities
16 such as Seattle, Oakland and San Francisco have found
17 this balance, and have recently passed and/or
18 introduced similar legislation. My hope from this
19 morning's hearing is to have a conversation with the
20 NYPD, many of our advocates, civil rights
21 organizations and other stakeholders about what the
22 NYPD can and should disclose and how we can
23 accomplish both safety and liberty simultaneously. I
24 want to thank the Administration, the NYPD and
25 everyone who is here to bring testimony today. I

2 look forward to a productive debate and conversation
3 on this very important issue through an open and
4 respected dialogue. I know that we can achieve an
5 understanding of how we can best address these
6 issues, and move forward with this POST Act. I'd
7 like to thank my colleagues who are here, and also we
8 will be joined by others, Council Member Robert
9 Cornegy, Council Member Rory Lancman, Council Member
10 Dan Garodnick, and Minority Leader Steve Matteo. I
11 also want to recognize the staff of the Committee on
12 Public Safety for their work, our Committee Council
13 Deepa Ambekar, Legislative Counsel Beth Golub,
14 Legislative Policy Analyst Casey Addison, Senior
15 Financial Analyst Steve Reister, my Chief of Staff
16 Dana Wax as well as Rob Newman for their work. I'd
17 like to recognize the prime sponsor of Legislation
18 Intro 1482 on today's agenda Council Member Dan
19 Garodnick.

20 COUNCIL MEMBER GARODNICK: Well, thank
21 you very much Chair Gibson for holding a hearing on
22 Intro 1482, which we are calling the POST Act, would
23 require that the New York City Police Department
24 publicly disclose on its website impact and use
25 policies about surveillance technologies that it's

2 currently using and plans to use in the future.

3 These policies must be posted for public comment

4 within 90 days of use with comments accepted for 45

5 days and final drafts of the policies posted no more

6 than 45 days after the comment period closes. The

7 NYPD has and should continue to have an impressive

8 capability for surveillance. We live in uncertain

9 times and surveillance is critical to their

10 operations and for keeping New Yorkers safe. But

11 civilians are in charge of the police force, and we

12 need to be able to understand what technologies are

13 being employed in our name. Unfortunately,

14 surveillance technologies are too often not only used

15 in secret, but they are acquired in secret. Even

16 local elected officials like us are kept in the dark

17 about what technologies the NYPD is buying and how

18 they're being used. A disclosure process for

19 surveillance technology would foster more public

20 trust in our law enforcement system. The POST Act

21 would require the NYPD to make clear their policies

22 related to new surveillance technology and to accept

23 feedback on its plans. It would give the public a

24 chance to engage substantively with the NYPD's

25 decisions regarding surveillance, and that public

2 feedback may actually help to expose weaknesses or
3 shortcomings in the PD's approach, and public
4 awareness of NYPD capabilities may also deter would
5 be criminals in the same way as does an officer's
6 physical presence on the street. It would also help
7 reassure New Yorkers that the city has sufficient
8 safeguards in place for sensitive information an era
9 of increasing hacks and data breaches. Finally, the
10 POST Act reinforces our commitment as a sanctuary
11 city by requiring that the NYPD disclose if any
12 outside entities including the State and federal
13 government have access to data collected by our own
14 local surveillance technology, and we understand the
15 Police Department has and will express concerns about
16 this bill, but we also know that these policies are
17 in place at the highest levels of the United States
18 government. The Department of Homeland Security has
19 a policy like this in place on its unmanned aircraft
20 systems. The Department of Homeland Security has one
21 in place for facial recognition at airports. The
22 Department of Justice has one in place on its
23 Stingray or Cell-Site Simulator Technology. This is
24 not without precedent. It is something that can be
25 achieved by the Police Department. What the bill

2 does not do is impact our ability for the police to
3 use the technology. We carefully crafted the bill so
4 that it does not require that the Police Department
5 disclose operational details regarding when and where
6 it will employ its tools. Let's face it, people
7 always learn about police surveillance tools
8 eventually. This bill gives the chance for the
9 public to engage with and even embrace this
10 technology, and it gives the police a chance to re-
11 examine their policies before everything inevitably
12 gets revealed in bits and pieces. This law
13 represents the best thinking for modern policing. I
14 look forward to hearing today's testimony. We look
15 forward to working the Police Department thoughtfully
16 on this bill. I encourage my colleagues to support
17 it, and to bring some real reform and transparency to
18 our surveillance tools here in New York City. Thank
19 you very much, Madam Chair.

20 CHAIRPERSON GIBSON: Thank you very much,
21 Council Member Garodnick, and now we will get to the
22 administration who is before us. Thank you to the
23 NYPD for your presence here today. We have our
24 Director Oleg Chernyavsky, our Deputy Commissioner
25 for Legal Affairs Larry Byrne, Deputy Commissioner

2 for Intelligence and Counter-Terrorism John Miller,
3 and our NYPD Chief of Detectives Chief Robert Boyce.
4 Thank you, gentlemen for being here this morning. We
5 look forward to your testimony, and now we'll have
6 our counsel administer the oath. Thank you once
7 again for being here.

8 LEGAL COUNSEL: Do you swear—do you
9 affirm to tell the truth, the whole truth, and
10 nothing but the truth in your testimony before this
11 committee, and to respond honestly to Council Member
12 questions?

13 DEPUTY COMMISSIONER BYRNE: I do.

14 LEGAL COUNSEL: [off mic] Thank you.

15 CHAIRPERSON GIBSON: You can begin.

16 Thank you.

17 DEPUTY COMMISSIONER BYRNE: Good morning.
18 My name is Larry Byrne. I'm the Deputy Commissioner
19 for Legal Matters at the New York City Police
20 Department. We welcome the opportunity to be here
21 today to testify about this proposed piece of
22 legislation. As we've said to you, Chairperson
23 Gibson and Councilman Garodnick in our previous
24 discussions and in our public discourse, we think the
25 drill—the proposed legislation as currently drafted

2 has fatal deficiencies, and we strongly opposed it in
3 its current format. What we would propose to do this
4 morning with your permission Chairperson as Chief
5 Boyce and Commissioner Miller will deliver some
6 opening remarks outlining our concerns about the
7 impact that this bill could have on investigating and
8 preventing traditional crime and preventing and
9 investigating potential acts of terrorism, and then
10 we're here to answer all of the questions of you and
11 your colleagues throughout the morning. So, if
12 that's acceptable, I'd like to turn it over to Chief
13 Boyce at this point or Chief of Detectives.

14 CHAIRPERSON GIBSON: Yes, thank you.
15 Good morning, Chief.

16 CHIEF BOYCE: A little more now-(sic) I
17 am Chief Robert Boyce, Chief of Detectives at the
18 NYPD. At the outset of our testimonies, I believe it
19 is important to stress that while conducting our
20 sensitive criminal and counter-terrorism operations
21 and deploying state-of-the art technology, the value
22 that the NYPD places on privacy rights and other
23 constitutional protections is paramount. The
24 protection of civil liberties is as important to the
25 Police Department as the protection of the city

2 itself. After all, it is these very freedoms that we
3 seek to defend against our adversaries. Our criminal
4 and counter terrorism investigations are treated with
5 particular care because we recognize that they may at
6 times implicate Fourth and Fourth Amendment and other
7 important issues. Accordingly, we abide not only by
8 the U.S. Constitution, and other applicable law, but
9 also in the case of counter-terrorism operations a
10 federal consent decree that compels additional checks
11 on our investigations. One of our many goals is
12 conducting criminal investigations just to strike the
13 appropriate balance between public safety with the
14 need to protect privacy rights. The NYPD Detective
15 Bureau is responsible for the prevention, detection
16 and investigation of crime and its efforts often
17 complement the hard work of the men and women of the
18 NYPD in each precinct. Detective work is highly
19 specialized usually encompassing the examination and
20 evaluation of evidence to apprehend suspects and to
21 build solid cases against them. The Bureau ensures
22 that each one of its commands conduct high quality
23 investigations in a timely manner, and that each
24 investigation is handled efficiently with dedication
25 and professionalism. The focus of the hearing today

2 is on surveillance technology utilized by the Police
3 Department. It should be no secret that the NYPD
4 investigators are trained to use a variety of
5 technology. What's important to underscore, however,
6 is that the purpose of using this technology is to
7 prevent, detect and investigate crime. Where this
8 technology intersects with legal expectation of
9 privacy, applications of court orders or warrants are
10 made to the District Attorney, which are then
11 submitted to—before a neutral judge. NYPD personnel
12 are trained in how to make these applications. Many
13 of the technologies utilized by our investigators be
14 it a wire tap, a panned register, a GPS tracking
15 device or any kind of technology that permits law
16 enforcement to listen to or gain the content of the
17 communication requires some kind of court order or
18 warrant. We do not begin investigations against
19 anything that would be purely constitutionally
20 protected activity. Likewise, we do conduct
21 surveillance in every case we investigate.
22 Surveillance is—is not an ominous exercise by the
23 local law enforcement. It is a routine of police
24 work. Our surveillance is triggered out of our
25 typical leads generated from the cases that our

2 personnel are investigating. All of our committees
3 under the Detective Bureau are responsible for
4 ensuring that where there is legal questions that
5 arise in the course of their investigations, that
6 personnel confer with the NYPD Legal Bureau and when
7 appropriate with the respective district attorney's
8 office, and the corporation counsel to properly
9 resolve any legal issues. The Fourth Amendment and
10 the State Constitution place a very high burden on
11 law enforcement. It should be a high burden. It
12 safeguards these civil liberties but also ensures
13 that investigator are properly managed and quality
14 arrests are being made. The stakes are too high if
15 we get it wrong. While Deputy Commissioner Miller
16 will opine more directly on several of the issues of
17 Intro 1482, I would like to highlight one area.
18 While perhaps in an effort to encompass future
19 technologies, the definitions of surveillance
20 technology is drafted so broadly that the strict
21 reporting requirements in the bill could be imposed
22 on non-germane technology. For example by defining
23 surveillance technologies, any equipment capable of
24 collecting location information the bill encompasses
25 technology used in our 9/11 system for emergency

2 response since it is often capable of tracking and
3 transmitting location information. This definition
4 would also encompass important technologies utilized
5 by the Department that protect public safety. This
6 legislation will require the Department to provide an
7 impact, a use statement of the department's
8 registered sex offender and gun offender tracking
9 systems. We would be obligated to publicly post a
10 detailed description of this technology and its
11 capabilities. Thereby, revealing the systems and
12 potential strength and limitations to those who would
13 be seeking to exploit this technology to avoid
14 registering altogether. Many of the current
15 technologies would also be implicated such as our
16 Domestic Violence Incident and Report Tracking
17 System. I will now turn it over to John Miller,
18 Deputy Commissioner of Intelligence and Counter-
19 Terrorism so that he may provide his remarks.
20 Following his remarks, I'll be glad to take any
21 questions. Thank you.

22 DEPUTY COMMISSIONER MILLER: Thank you,
23 Madam Chair and members of the committee. More than
24 any other place in the world, New York City remains
25 in the crosshairs of violent terrorists. Since

September 11, 2001, there have been in excess of 21 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 Federal Reserve, 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 partners in the FBI and the JTTF. We have been able to build a deterrent that has kept the city safe while protecting and upholding 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 simply defer the responsibility of protecting the city from terrorist attacks to others that we had to be as police department a full and active participant, and we've continued to prioritize this ever-evolving menace. Soon after 2001, the NYPD became the Fourth police department in the country to develop its own robust counter-terrorism capacity. We established a division for training and equipping every one of our police officers for a counter-terrorism mission. We

2 changed our intelligence operations to have a new and
3 international focus. Our mission now includes
4 gathering and analyzing intelligence with global
5 implications. Our commitment to ensuring that
6 sufficient resources are dedicated to this critical
7 mission has not changed. One of the premier
8 resources is our personnel. Over the years the
9 caliber of people we've been able to attract and
10 recruit has played a major role in our ability to
11 protect New York City. We have hired civilian
12 analysts who are experts in intelligence and foreign
13 affairs. They studied terrorist groups, trends and
14 methods of attack. Moreover, one of our most
15 important institutional strengths is the remarkable
16 diversity of our ranks. The NYPD is fortunate to
17 have a deep pool for foreign speaking officers. This
18 has allowed us to build a foreign linguist program
19 with more than 1,200 registered speakers of 85
20 different languages: Arabic, Dari, Farsi, Mandarin,
21 Pashto, Russian, Spanish and Urdu, just to name a
22 few. From counter-terrorism to crime fighting to
23 community relations through our Community Affairs
24 Bureau we have assigned liaisons to the Arab, Muslim,
25 Chinese, and Eastern European, Hispanic and West

2 African communities. We are also exceptionally proud
3 of our over 1,000 Muslim officers who are a vital
4 part of this department, its diversity and these
5 efforts. Technology is also critical. In an
6 unprecedented initiative supported by the Department
7 of Homeland Security we have installed radiation
8 detection equipment throughout neighboring
9 jurisdictions surrounding New York City at key points
10 of entry into the five boroughs so that the city is
11 virtually ringed with an alarm system. This program
12 know and securing the cities includes 150 different
13 law enforcement agencies and dozens of nearby cities
14 and towns. The NYPD has been responsible for
15 distributing all of the radiation detectors used by
16 our partners. When it comes to the private sector,
17 we collaborate with nearly 18,000 members of the
18 region's private security industry through a program
19 called NYPD Shield. The membership consists of
20 security professionals tasked with protecting
21 critical infrastructure in sensitive buildings in the
22 New York Metropolitan area. Through the Shield
23 Program, we regularly host conferences, sector
24 specific briefings and training seminars as well as
25 Share NYPD strategic assessments on terror trends.

2 Under another initiative known as the NEXUS Program,
3 our detectives have made visits to businesses that
4 make, sell or inventory products that could be useful
5 materials in plotting a terrorist attack. This is a
6 location such as truck rental outfits, fertilizer
7 stores, and chemical supply companies. We asked them
8 to contact us if they see anything suspicious or
9 anything that gives them pause. We also partner with
10 the private sector to secure areas of the city known
11 to be terrorist focal points. We do this through the
12 Domain Awareness System or DAS. It's a centralized
13 network of security cameras, License Plate Readers
14 and chemical and radiological detectors. Using an
15 advanced graphic user interface and mapping
16 capability, the DAS is able to retrieve and display
17 information to provide real time alerts and the means
18 to quickly call up relevant information to guide
19 police action. This makes it possible for us to scan
20 recorded footage for specific objects and behaviors.
21 We can also program the system to alert us to
22 potentially suspicious scenarios whether that's a bag
23 left unattended in front of a secure location, or a
24 car driving against the flow of traffic or a person
25 walking through a restricted area. The program

2 receives data from more than 6,000 cameras, nearly
3 500 License Plate Readers and scores of strategically
4 chemical and radiation detectors throughout the city
5 that provide instant alerts on possible threats to
6 New York City. Since it is an available—since it is
7 available as an application on the Police
8 Department's Smart Phones, the features of the DAS
9 system are available at the fingertips of all our
10 officers. The privacy policy for this system, was
11 posted before the system was activated, and the
12 system after—after leaving that policy out there for
13 public comment, was actually built to the policy and
14 lives and operates within those limits. This was
15 done voluntarily and proactively by the Police
16 Department. Across the city we've distributed
17 approximately 3,000 radiation pages. These units are
18 throughout the department. We've also distributed
19 nearly 4,000 radio active densitometers to each
20 patrol borough's counter-terrorism trailers. We
21 continue to invest heavily on acquiring and
22 maintaining state-of-the-art equipment to identify,
23 prevent of disrupt terrorist threats. From sonar
24 systems to thermal imaging cameras we've installed
25 highly sensitive detection equipment on the boats,

2 helicopters and aircraft we use to patrol New York
3 Harbor. Police vehicles area also outfitted with
4 similar detection capabilities. We're also
5 constantly looking to disrupt any budding or nascent
6 plots to attack New York City. Everyday through
7 Operation Hercules, we deploy teams of heavily armed
8 officers to make unannounced visits to iconic
9 locations and potential targets. We stage multiple
10 critical response command vehicle deployments
11 throughout the city that arrive sometimes in
12 formation with lights flashing to pre-arranged
13 locations. You will see as a result of the shootings
14 in Virginia today the critical response command
15 personnel have been moved to City Hall and other
16 government buildings to enhance protection until we
17 understand what more is behind that incident as well
18 as some of the public events that members of the
19 Council and other officials are attending today. We
20 have similar units that focus on ferry terminals,
21 regional transport lines and the subways. We place
22 particular emphasis on the subway system in light of
23 its primacy as a target and because it's a vital
24 artery that keeps the city running. An excess of
25 five million New Yorkers use the subways everyday.

2 Protecting the system is one of our top priorities,
3 and one of our greatest challenges. That's because
4 the entire system is designed to be open 24 hours a
5 day, everyday of the year. Its very strengths as a
6 mass transit artery makes it an attractive target for
7 potential attackers. After the bombing of the London
8 Transit System in 2005, the NYPD began screening bags
9 and backpacks of subway passengers at random
10 locations, and at different times. Everyday we
11 maintain posts at each of the 14 underwater subway
12 tunnels. We have heightened the uniform patrols and
13 underground and con-underground and conduct regular
14 security sweeps of subway cars. These are just some
15 of the tools we're using to keep pace with the
16 evolving threat of terrorism. The philosophy behind
17 them is simple, we have to develop the best
18 intelligence available, expand our partnerships and
19 take protective measures to defeat whatever our
20 adversaries might be planning next. Unfortunately,
21 our adversaries have multiplied in recent years.
22 What was once the domain of only a few top-down
23 hierarchal organizations operating from safe havens
24 overseas of failed and hostile spaces has overtime
25 developed into regional affiliates and local upstarts

2 dispersed across the globe as well as entrepreneurial
3 lone wolves within our shores dedicated to
4 actualizing our adversary goals. There have been
5 multiple calls for violence against New York City.
6 In 2014, the twelfth issue of Inspire Magazine, the
7 prominent English language magazine as Al-Qaeda's
8 Yemen based affiliate, Al-Qaeda in the Arabian
9 Peninsula, urged lone wolf car bombs attack—car bomb
10 attacks in U.S. cities while specifically mentioning
11 the Queens based U.S. Open as a desirable target. A
12 November issue of Ramia Magazine, published by ISIS
13 last year, urged attacks against the Thanksgiving Day
14 Parade. A more recent issue of Ramia Magazine
15 suggested tactics for taking hostages in U.S. cities,
16 kidnapping people, stabbings and shootings. There
17 are also reports that ISIL and Al-Qaeda operatives in
18 Syria and Iraq have continued to plot against the
19 homeland. In addition to monitoring potential
20 threats abroad, we have to be concerned about the
21 threats originating right here at home. Last year we
22 witnessed the horrifying terrorist attack that took
23 place in Orlando, Florida. While I'm sure this body
24 needs no reminders about that event, the city itself
25 was—this city was the recipient of a terrorist attack

2 in—in the form of the Chelsea bombing on September
3 17th. That attacker had planed this attack for
4 months, and took inspiration from Osama Bin Landen
5 and the leader of ISIS. Last week to covert operative
6 officers working on behalf of the Iranian backed
7 group Hezbollah were charged in New York City
8 undergoing weapons training, and the conducting pre-
9 operational surveillane of potential targets for
10 terrorists to attack including locations in Manhattan
11 not far from this building we are sitting in right
12 now in Brooklyn just across the bridge and both New
13 York City airports.

14 Now, turning to the legislation under
15 consideration today, Intro 1482, would require the
16 reporting and evaluation of surveillane technology
17 used by the NYPD. Under this proposal, the
18 department would be required to issue a surveillane
19 impact and use policy about these technologies and
20 would include information such as its description and
21 capabilities as well as rules, processes and
22 guidelines, and any safeguards and security measures
23 designed to protect the information collected. Upon
24 publication of the draft Surveillane Impact and Use
25 Policy, the public would have a period of time to

2 submit comments. The Police Commissioner would have
3 to consider these comments, and provide the final
4 version of the Surveillance Impact and Use Policy to
5 the Council, the Mayor and then post it to the
6 department's website. Further, the NYPD Inspector
7 General can audit the Surveillance Impact and Use
8 Policy to ensure compliance with the bill. While I
9 will reiterate that the department is committed to
10 transparency as a principle, we are also mindful of
11 maintaining the appropriate balance between
12 reasonable transparency and still having the
13 effective tools and technologies needed to protect
14 our city. This proposal would require us to
15 advertise sensitive technologies that criminals and
16 terrorists do not fully understand it would require
17 the Police Department to list them all in one place,
18 describe how they work, what their limitations are
19 that we place upon them, and our use of them. In
20 effect, it would create a one-stop-shopping guide to
21 understanding these tools and how to thwart them for
22 criminal elements and terrorists across the nation or
23 the world, depending on who decided to access this
24 site and study it. The department absolutely opposes
25 this proposal, as it is written too broadly to be

2 practical. More specifically, this proposal would
3 require the Police Department to provide an Impact
4 and Use Report disseminated online for each piece of
5 equipment deemed surveillance technology, and provide
6 a detailed description of the technology and its
7 capabilities. In addition to the examples I provided
8 in my testimony, the tragic events that have taken
9 place today in Alexandria, Virginia, the events in
10 the United Kingdom over the last several weeks remind
11 us that the threat from terrorists or active shooters
12 is indeed real and persistent. A public
13 advertisement detailing the type and quantity and
14 other—other specifications of technology and
15 equipment would one report by another report reveal
16 the strengths and potential limitations of the
17 department's counter-terrorism defense operations to
18 any terrorist or criminal organization doing its due
19 diligence. In many ways, producing these reports
20 undermines the security strategy and the technology
21 that it intends to support. This is not a passing
22 objection. Terrorists and criminals do their due
23 diligence, and they literally study and adapt to
24 evolving security measures. Terrorists and criminals
25 constantly revise their trade craft to reflect new

2 intelligence, leak classified information, publicly
3 available information and lessons learned from
4 previous operations have provided valuable insight
5 for terrorist groups and criminal enterprises into
6 government surveillance and detection methods. Based
7 on these sources, terrorist groups have been creating
8 formal and informal guidance for their would-be
9 followers for years even before the rise of ISIL.
10 For example, the Manchester papers, the so-called Al-
11 Qaeda Manual, which was discovered in 2000, provided
12 tactical guidance for trained operatives based on
13 knowledge of how law enforcement operates. More
14 recently, ISIL and its supporters have published
15 multiple tactical guides some with information on
16 specific devices as well as detection on how to evade
17 camera based technology. In recent—the recent
18 increased focused on small scale low-attack attacks
19 by terrorists organizations, is also a response to
20 greater understanding of how government disrupts
21 plots. This is the new emphasis by ISIL and other
22 organizations on knife attacks or car ramming plots
23 or active shooter scenarios. More generally, though,
24 the types of guidance we see and the attacks that we—
25 that have ensued across the western world recently

2 are responses to a better understanding of the
3 government's playbook *Writ Large*. Terrorist
4 organization are not the only ones who could exploit
5 this information. Hackers would also welcome this
6 information. Municipal systems have been targeted in
7 the recent past by hackers exploiting security
8 vulnerabilities. This past January, 123 of
9 Washington, D.C.'s 187 police cameras were infected
10 with Ransomware, a malicious software that blocks
11 access to critical data until a ransom is paid. As a
12 result of that cyber attack the, infected cameras
13 were unable to record between January 12th and
14 January 15th. The issue was ultimately resolved by
15 manually removing the software from each infected
16 device and restarting the entire system. I provide
17 these examples because one of the perhaps unintended
18 consequences of the proposed legislation as written
19 would be that with more knowledge of city systems
20 vulnerabilities can come to light and be exploited by
21 those seeking to do harm. Anyone looking to conceal
22 activities will be exploit vulnerabilities—
23 vulnerabilities in government programs to design—to
24 design tactics. This legislation would created an
25 effective blueprint for those seeking to do harm.

2 Other issues also exist with this legislation. The
3 requires that the department disclose in each impact
4 and use statement whether other local, state, federal
5 or private entities have access to the information
6 collected from the surveillance technology. We have
7 concerns that publicly disclosing sensitive
8 information such as this could potentially chill our
9 ongoing relationships with vital law enforcement
10 partners. Part of the city's success in thwarting
11 potential terrorist attacks stems from our solid
12 relationship with local, state and federal partners.
13 It is also unclear how this legislation is compatible
14 with the state's Freedom of Information Law.
15 Producing reports required in this legislation could
16 reveal non-routine investigative techniques possible
17 in fair, present or imminent contract awards or
18 reveal critical infrastructure. This is all
19 information that is wisely exempted under FOIL.
20 Furthermore, the bill requires that prior to the use
21 of new technology, the impact and use statement must
22 be posted 90 days in advance and a 45-day period for
23 the public to submit comments to the Police
24 Commissioner must also be permitted for each report.
25 The Police Commissioner is to consider these comments

2 and finalize this report. The department is also to
3 amend any impact or use statement when enhancement
4 for the current technologies are sought. This is an
5 unprecedented hurdle placed on a singular agency.
6 Often the technology sought in this legislation is
7 needed imminently and legislation would impede the
8 department's ability to evolve with critical
9 technology based on the changing circumstances of the
10 threat. Proponents of this bill assert that there is
11 a need for this legislation out of concerns for local
12 transparency and oversight. In considering the
13 amount of public reporting conducted by this agency,
14 which is done either voluntarily or pursuant to law,
15 as well as the amount of datasets that we release
16 each year online, the number of FOIL requests
17 received and responded to and the fact that our
18 patrol guide is now publicly available online with
19 only the most minor redactions pursuant to a bill
20 sponsored by Council Member Garodnick and supported
21 by this department. The New York Police Department
22 is the most transparent municipal police department
23 in the world. Over the last several years, the
24 department has regularly worked with and negotiated
25 with the Council on a number of pieces of legislation

2 that provide valuable data to the public and the
3 advocacy community, a broad categorization that the
4 department is not transparent would be simply false.
5 Part of being transparent is to continually improve
6 trust with communities. For this subject a
7 particular emphasis is placed on communities most
8 affected by the issue of terrorism. Personnel from
9 out Intelligence and Counter-Terrorism Bureaus as
10 well as our Community Affairs Bureau regularly meet
11 with religious and community leaders to discuss
12 potential threats concerning trends and fears that
13 their community share. The exercise of oversight is
14 robust—is robust. The court system is indeed
15 providing effective oversight of the NYPD's
16 Intelligence and Counter-Terrorism Initiative. As
17 you know, the department operates within the Handschu
18 Guidelines, which specifically promulgate how an
19 investigation can be launched and governs the NYPD's
20 investigation of political activity including
21 terrorist related crimes. Recently, as a result of
22 settling ongoing litigation, the department has
23 agreed to install a civilian representative in its
24 internal Handschu Committee, which reviews
25 investigations prior to final action by the Deputy

2 Commissioner of Intelligence. This representative
3 who was a former U.S. District Court Judge Stephen
4 Robinson is appointed by the Mayor and has the
5 ability to review, monitor—and monitor compliance
6 with all provisions of the Handschu Guidelines.

7 Moreover, the civilian representative is given
8 unfettered access to the courts to communicate any
9 concern arising out of his function on the committee.

10 More locally, the department is subject to oversight
11 of the NYPD Inspector General and the City Council.

12 In 2014, testifying before this committee on the
13 city's emergency preparedness, we discussed many of
14 the technologies that would be subject to this
15 legislation. As a department we're always willing to
16 engage in substantive discussions with the Council,
17 the advocacy community and the public on a variety of
18 topics, and it is not secret that representatives
19 from this department regularly participate in several
20 Council hearings each month. It would also be an
21 oversight not to mention the very capable works of
22 the attorneys of the department's Legal Bureau, which
23 providers' guidance on the constitutionality of
24 specific techniques whether we are striking the
25 approach—and whether we are striking the appropriate

2 balance between security concerns and civil
3 liberties. The NYPD's Legal Bureau has several
4 attorneys specifically assigned to handle
5 intelligence and counter-terrorism issues, and the
6 Deputy Commissioner of Legal Matters plays a vital
7 role on our Handschu committee. While legislation
8 similar to this proposal has been enacted in other
9 jurisdictions, it is fair to say that none of these
10 jurisdictions are the number one target for
11 terrorists worldwide. That is not speculation. It is
12 the consensus of the Global Intelligence Community
13 and statistically proven by the number of plots
14 targeting a single city. Furthermore, although
15 federal agencies are obligated to submit privacy
16 impact assessments on their information technology
17 pursuant to the E-Government Act of 2002, these
18 federal requirements are distinguishable from the
19 bill under consideration today. Most notably, the
20 federal law does not require publicizing privacy
21 impact assessments for technology and systems, which
22 involve among other things sensitive information that
23 could potentially damage law enforcement efforts, but
24 raise security concerns. Federal law requires impact
25 assessments throughout multiple federal agencies and

2 encompasses systems and equipment used throughout the
3 country. This bill focuses on one agency and
4 essentially is so localized that it provides a
5 particularized list of critical technology and
6 equipment used to defend and protect a single
7 jurisdiction. In the final analysis, all that this
8 legislation does is provide an invaluable road map to
9 terrorists, criminals and others on how to more
10 effectively harm the public, commit crimes and hurt
11 the interest of our city. Over 15 years since 9/11,
12 New York enjoys the distinction of being the safest
13 big city in America. It is also a commercially
14 vibrant, culturally diverse and free. We can claim
15 these successes are due in no small measure to the
16 50,000 plus uniformed and civilian members of the
17 NYPD in cooperation with our local and state and
18 federal partners who have demonstrate initiative and
19 perseverance in the face of varied and continuing
20 threats. Thank you again for this opportunity to
21 testify today. As with Chief Boyce, I am happy to
22 answer any questions.

23 CHAIRPERSON GIBSON: Thank you very much,
24 Chief Boyce. Thank you Commissioner Miller, and
25 thank you Deputy Commissioner Byrne and—and Director

2 Oleg. I appreciate your remarks and your testimony.
3 I also want to acknowledge we've been joined by
4 Council Member Vincent Gentile and Council Member
5 Chaim Deutsch, and Commissioner, in your testimony
6 you provided a very detailed description of the
7 technology that's being used by the department, a
8 number of the terrorist efforts that obviously have
9 been plotted against us that we have successfully
10 prevented. The work you're doing with clergy and
11 faith-based organizations and the engagements with
12 many in vulnerable communities, and I guess overall,
13 I appreciate all of the work that is being done. I
14 don't think every New Yorker recognizes the threat
15 that we are under everyday, and in my travels
16 throughout the city I've seen SRG and CRC and many of
17 the high visibility points around Times Square and
18 parts of my district in the Bronx, and I guess what
19 I'm trying to understand, and the first question I
20 want to ask is with all of the technology and
21 surveillance equipment that the department uses that
22 you even described in your testimony. The City
23 Council doesn't get any of that information. None of
24 it is shared with us through any formal or informal
25 process. So, if we were to ask the department for

2 information I'm sure that you would comply, but while
3 we're working together, there's no formal process, no
4 formal agreement that we have on receiving any
5 information on the technology and the equipment
6 that's used by the department. So, I guess this bill
7 and today's hearing really stimulating for many of us
8 a very important conversation that we probably should
9 have had some time ago, but now we're having it
10 today. So, what I'd like to understand is all the
11 information that you've shared, what is it that you
12 can officially share with the City Council that would
13 be helpful to us to continue to build this
14 relationship?

15 DEPUTY COMMISSIONER BYRNE: I would start
16 off by underlining that the larger system involved
17 here that has cameras in public places, some of them,
18 if they're NYPD cameras are labeled and conspicuous.
19 Many of them are private cameras that through
20 individual agreements with entities we're able to
21 capture and record from as well as personally
22 identified information is the Domain Awareness
23 System, and that is where the department proactively
24 developed a privacy policy, put it up for public
25 discussion and it remains posted in fairly intimate

2 detail on the New York City website for any member of
3 the Council or any member of the public to see. So,
4 that's at the highest level of a system that collects
5 a lot of information and is used everyday in
6 thwarting crimes, and protecting the city from
7 terrorism. The greatest concerns here are about the
8 narrowing of that scope to the kinds of equipment
9 that are used in authorized investigations against
10 specific targets who may be a single individual or a
11 small group of individuals who are plotting terrorist
12 attacks or activity in New York City. The way this
13 bill is written right now it would be asking us to
14 say describe the manufacture type and capabilities or
15 recording devices worn by undercover officers or
16 other human sources who were in the middle of an
17 ongoing terrorist plot. That would be insane. So, I
18 think somewhere in between the broader information
19 collection and exploitation efforts of the NYPD like
20 the DAS System where we've been very proactive and
21 the bottom, which is very specific and could endanger
22 lives not just of citizens, but also of police
23 officers. There is a logical discussion to be had
24 short of this bill as it is currently written.

2 CHAIRPERSON GIBSON: Okay, and I
3 appreciate that.

4 DEPUTY COMMISSIONER BYRNE: I'd like to
5 just—I'd like to just add to that because we've heard
6 a lot this morning on this discussion about privacy
7 and privacy interests. Let's talk in the big picture
8 for a minute about privacy interests vis-à-vis what
9 happens in public and what happens in a private place
10 and how we utilize different technologies in those
11 instances. You mentioned License Plate Readers, and
12 you mentioned another technology, which I'll think of
13 in a minute. Those capture things that happen in a
14 public place. If you choose to driver your vehicle
15 across the Queens Borough Bridge into Manhattan or
16 through the Holland Tunnel into Lower Manhattan, you
17 have no privacy interest in that movement. Courts
18 have ruled that. There's no Fourth Amendment
19 interest. If you choose to go out for a lunchtime
20 walk in front of Goldman-Sachs on West Street and
21 they capture you walking down the street, you have no
22 privacy interest in that, and for that reason we have
23 no requirement to get a court order to look at what
24 happens open and in public. If we choose as part of
25 an authorized investigation to, for example, use

2 Cell-Site Simulator Technology, which our technology
3 does not intercept the content of communications. It
4 gives us the location of a person under
5 investigation. We do that pursuant to a court order
6 based on probable cause. If we choose to intercept
7 the content of your electronic or wireless
8 communications, emails, text, cellphone, we do that
9 pursuant to a court authorized order with all
10 restrictions overseen by a judge and a district
11 attorney and a prosecutor. So, I think if you cut
12 through the privacy concerns, which we acknowledge
13 are very valid and have been very sensitive to over
14 the years, we have to distinguish between what
15 happens in public and what happens in private. And
16 when we're looking at things with various
17 surveillance technologies in private, we're doing it
18 pursuant to a variety of court orders whether it's a
19 search warrant, whether it's an interception warrant,
20 whether it's a Cell-Site Simulator warrant supported
21 by probable cause, approved by an independent judge
22 and prosecutor. I think it's important that we get
23 that into the record today.

24 CHAIRPERSON GIBSON: Okay, and without
25 probable cause, how long is the data maintained in

2 your system? So, if you're tracking emails, the
3 License Plate Readers is it accurate that the data is
4 maintained for up to five years. So without probable
5 cause, is this data kept on file for the department
6 to view?

7 DEPUTY COMMISSIONER BYRNE: [off mic]
8 I'm sorry, did you say tracking emails?

9 CHAIRPERSON GIBSON: License Plate
10 Readers. Larry, you just mentioned emails. No,
11 John, I'm sorry. (sic). I'm, sorry.

12 DEPUTY COMMISSIONER BYRNE: [interposing]
13 Yeah, when we intercept the content of emails, that's
14 pursuant to a court order.

15 CHAIRPERSON GIBSON: Okay.

16 DEPUTY COMMISSIONER BYRNE: And when we
17 intercept stuff pursuant to a court order, it's part
18 of an investigation.

19 CHAIRPERSON GIBSON: Okay.

20 DEPUTY COMMISSIONER BYRNE: That
21 investigation may result in charges and it may not,
22 but how we treat that data, store that data and who
23 has access to that data, is defined in part by the
24 court order, and is overseen by the judge. So, when
25 we do electronic interceptions of emails or cell

2 phone conversations, pursuant to court order, we are
3 prohibited from publicly disclosing that. We can use
4 it for investigative techniques, and when we bring
5 charges, we then can unseal that evidence and turn
6 it-over to the person's attorney intercepted for the
7 defense of their case. But investigations continue
8 both criminal investigations and terrorist
9 investigations continue for long periods of time.
10 Remember that murder in New York State has no statute
11 of limitations. We are solving-Chief Boyce's
12 detectives almost every month a homicide from 15, 20,
13 25 years ago as new information becomes available, as
14 new witnesses become available, and yes as new
15 technology becomes available, whether it's DNA
16 technology or other issues. So, how we treat, store
17 and retain investigative material whether it's
18 pursuant to court order or whether it's pursuant to
19 open source material is overseen within the
20 department for things like License Plate Readers and
21 the private camera system. There is only so much
22 storage capability for a certain period of time, and
23 so it would vary by technology. We would have to
24 break that down for you after that hearing for what

2 the retention periods are absent an intervening event
3 like a criminal prosecution or a civil lawsuit.

4 CHAIRPERSON GIBSON: Okay, and—and that's
5 my question. Absent of the ongoing investigations
6 and solving crimes, I'm talking about the equipment
7 that's used on everyday New Yorkers. As you
8 mentioned, driving your car across a city bridge on a
9 city street, you know, there are no privacy laws that
10 would protect you. So, with the License Plate
11 Readers that data is stored in a database, and I'm
12 trying to understand the length of time that it's
13 kept on record and absent of a criminal
14 investigation, absent of a court order how long is
15 that data kept and is it used for other things?

16 DEPUTY COMMISSIONER BYRNE: That is
17 posted on the website. We have cited the period for
18 License Plate Readers. It's different for video, but
19 that has all been made public, and was made public
20 before the system was enacted, and—and reviewed by
21 the public. Public comments were accepted in review
22 and the system was built to those specs.

23 DEPUTY COMMISSIONER MILLER: And let me
24 give you the most recent example of how License Plate
25 Readers could have been a critical tool. Any time a

2 vehicle is stolen in New York City, we immediately
3 post an alert through License Plate Readers, and
4 officers in precincts will get alerts when that
5 stolen vehicle happens to be in their area, and is
6 picked up by a License Plate Reader. The car that
7 dragged Officer Veve over 1,000 feet, critically
8 injuring him, as he fights for his life in the
9 hospital today, was a stolen vehicle. It was stolen
10 in Nassau County. Because it was in another
11 jurisdiction, there was a lag time in how it got
12 posted to our system. That's no one's fault, but the
13 fact is we were able to after the tragedy track the
14 movements of that vehicle from when it was stolen to
15 when he was critically injured. That's one example
16 of how that tool was used, and why the information
17 needs to be retained.

18 CHAIRPERSON GIBSON: Okay.

19 CHIEF BOYCE: Just if I could also add
20 the Times Square individual who ran down those people
21 as well, we were able to track his movements by going
22 back on his license plate. [coughs] It's when he
23 entered the city that day, and what his whereabouts
24 were prior to that. Key information that went into
25 that case.

2 CHAIRPERSON GIBSON: Okay, and I guess
3 what I'm also trying to understand and, you know,
4 you're highlighting all of the cases obviously that
5 were horrific and could have been much more worse if
6 you didn't use the equipment that you have, but
7 ongoing as you look at increasing technology and
8 access to better equipment that can allow you to do
9 your work better, you know, do you not believe that
10 the public has a right to understand some of the
11 technology that you're using and what it's used for?

12 DEPUTY COMMISSIONER MILLER: I-I think
13 that--that I would refer to my earlier answer, which
14 is in the broader systems, this is something that is
15 certainly worth discussing with the Council--

16 CHAIRPERSON GIBSON: Right.

17 DEPUTY COMMISSIONER BYRNE: --on a bill
18 that would make sense, but the bill as written covers
19 not just systems that retain information, but it is
20 specifically written and targeted to reveal and
21 discuss in public not just our broader information
22 gathering efforts, which we've already disclosed
23 proactively, but very sensitive surveillance
24 equipment that are used on the persons of police
25 officers during undercover operations and--and

2 locations during authorized investigations sometimes
3 subject to court order, and as written, again it
4 would endanger police officers' lives, or the lives
5 of other human sources, and the lives of citizens who
6 may be caught in either criminal activity or
7 terrorist attacks that are then not thwarted because
8 our adversaries and terrorist groups or criminal
9 organizations understand more about this. As it is,
10 the study of law enforcement's ability to gather
11 information during authorized investigations has
12 spawned an industry where terrorist organizations
13 have obtained and used daily as well as criminal
14 organizations and violent gangs, encrypted
15 applications and locked cell phones that cannot be
16 accessed even with court orders and search warrants.
17 Now, this threatens to expand on the knowledge that
18 would counter these technologies in a way that is
19 extraordinarily concerning to me and the people of
20 the Intelligence and Counter-Terrorism Bureaus.

21 CHAIRPERSON GIBSON: Okay. In your
22 testimony you alluded that there are things that you
23 would be willing to agree with us on outside of the
24 written bill itself, and I think in Chief Boyce's
25 testimony or yours, you gave some individual

2 examples, the domestic violence system itself where
3 there could be sensitive information. You know, even
4 with the Patrol Guide being online now, there are
5 parts of that that are redacted, and when we started
6 the conversation on the Patrol Guide being online, we
7 didn't necessarily agree, but we found common ground.
8 So, what I'm hoping that and through this hearing and
9 even conversations we're having after there is
10 information that the department is willing to share,
11 and obviously without compromising public safety. I
12 have two questions that I wanted to ask about the-
13 obtaining a warrant in and a court order, betting it
14 approved by a judge. Who determines the threshold of
15 the amount of information that you have to gather to
16 produce and get a warrant signed off by a judge, and
17 is there an internal that the department has for all
18 of your equipment, or is it delineated by the type of
19 equipment you use.

20 DEPUTY COMMISSIONER BYRNE: When we're
21 going to get a court order from a judge whether it's
22 a search warrant, whether it's a court order to use
23 Cell-Site Simulator Technology, and again, our
24 technology that we use does not reveal the content of
25 communications. It reveals the location of the

2 person whether we're getting a surveillance order to
3 intercept the content of communications. Courts have
4 established the standard for decades. The standard
5 is we have to show probable cause to believe that by
6 getting this order we will be able to uncover
7 evidence of ongoing or past criminal activity.
8 That's a well established legal principle. Every
9 detective in the Detective Bureau receives legal
10 training on that, and the legal, I mean the Detective
11 Bureau, and the entire department in this academy and
12 in promotional classes. When it comes time in an
13 investigation to get a court order, it has to be
14 supported by an affidavit, which establishes probable
15 cause. That is drafted and presented to a
16 prosecutor, and a prosecutor then in turn takes that
17 to a judge and the judge will review it and she will
18 say, you have probable cause, here's your order or
19 you don't have probable cause, you don't have
20 probable cause, you can't do that, and we will abide
21 by that decision. That is a well established
22 practice that's been going on for decades. It works
23 and it means that our oversight of technologies and
24 investigative techniques every day is being overseen

2 by state and federal judges in the five counties of
3 this city.

4 CHAIRPERSON GIBSON: Okay, and taking it
5 a step further, does the department have internal
6 protocols that detectives have to follow in order to
7 use some of this equipment in their investigations?

8 CHIEF BOYCE: Yes, we do. We have an
9 oversight for like the investigation squad. If
10 there's an issue we look at it. All my supervisors--
11 most chiefs are trained in reviewing cases. There
12 are--are dedicated on what we call DD5s, Detective
13 Division 5s within a case folder. They are read and
14 signed off by supervisors. So, each step along the
15 way a sergeant, lieutenant and then captain in my
16 instances and even chiefs in some big cases will read
17 the case and reads the investigative steps on each
18 way.

19 CHAIRPERSON GIBSON: Okay, and what
20 happens if--if the--if the investigation itself--I think
21 Larry talked a little bit about that. If it extends
22 over a period of time, does that authorization by
23 that supervisor, that sergeant or lieutenant does
24 that carry for the entire investigation? What
25 happens if you're using it one time and then six

2 months later you have to go back and use it again to
3 gather more evidence on top of--

4 CHIEF BOYCE: Generally speaking, it's
5 specified in the warrant, and I also want to say if
6 it's a phone tap is a 30-day--normally a 30-day review
7 by a judge. That is--

8 CHAIRPERSON GIBSON: [interposing] Okay,
9 that's what I was asking.

10 CHIEF BOYCE: --that is done. This gets
11 done all the time. The detective with the District
12 Attorney goes back in front of the judges and either
13 says we don't need any more or we need more time to
14 do it.

15 DEPUTY COMMISSIONER BYRNE: And to
16 amplify that point, and Chief Boyce is absolutely
17 right, so a search warrant whether it's to search
18 physical premises or the content in an electronic
19 device has a return date. If the search warrant is
20 not executed within that return date--which is
21 usually a short period, often seven days or less--we
22 have to go back before the judge and re-establish
23 probable cause, or we can't execute on that warrant.
24 Intercepting the content of communications is
25 generally subject to a 30-day limitation, and then we

2 have to re-establish every 30 days that probable
3 cause still exists. So, there are very strict
4 safeguards around how long and how these technologies
5 can be used under court supervision.

6 CHAIRPERSON GIBSON: Okay. At an earlier
7 hearing we were talking about immigration and the
8 NYPD's relationships with other law enforcement
9 agencies. I wanted to further understand the data
10 sharing. Does the department share any data that you
11 collect through surveillance technologies with other
12 agencies, and how does that work with your
13 relationship with other law enforcement?

14 CHIEF BOYCE: Well, I will say City
15 Council that we have federal taskforces that
16 investigate gangs and narcotics in that space and at
17 given times they are investigating different groups
18 through the city. That is shared with our—with our—
19 with our agencies as Memorandum of Understandings
20 clearly delineating what information goes back and
21 forth between two agencies. That is the only time
22 that I can think of at this point in the Detective
23 Bureau that we deal with outside agencies.

24 DEPUTY COMMISSIONER BYRNE: On the
25 Intelligence and Counter-Terrorism side, our

2 officers, over 100 detective and police officers who
3 are assigned to the FBI's Joint Terrorist Taskforce,
4 actually operate as deputized federal agents and
5 operate under—they operate as federal—they operate as
6 federal agencies pursuant to the Attorney General
7 Guidelines and the FBI's Domestic Intelligence
8 Operations Guide. So, those are the rules they
9 follow since many of the other law enforcement
10 agencies are part of that taskforce. They're all
11 going from the same book. The AG Guidelines are very
12 similar certainly in principle if not in form with
13 the Handschu Guidelines. As far as sharing
14 information from systems, within the Domain Awareness
15 System, information can or may be shared, but only
16 with the approval of the Deputy Commissioner of
17 Counter-Terrorism or the Chief of Counter-Terrorism.
18 So, there is oversight in sharing, legitimate sharing
19 of information with other law enforcement agencies as
20 we have to share with them. As you know, because I-I
21 think this question has a tale. As it comes to
22 immigration matters and other things we have a
23 separate policy as thee NYPD about what--what
24 information is shared, much of that pursuant to City
25 Council legislation.

2 DEPUTY COMMISSIONER MILLER: And as I've
3 testified previously, we do not engage the NYPD in
4 civil immigration enforcement. We are not a
5 surrogate agency of ICE. We have adhered as I
6 testified to recently scrupulously with the City
7 Council bill governing detainers and honoring
8 detainers. As a general matter and I think we should
9 step back, we are a law enforcement agency. We're,
10 in fact, the leading law enforcement agency in the
11 country if not the world. That means we are doing
12 confidential investigations everyday of criminal
13 activities and of terrorist activities, and we
14 collect that information whether it's an interview
15 that gets written up in a DD5 and put in a file, a
16 photograph that's taken, a communication that's
17 intercepted. We guard the confidentiality and
18 integrity of that data with great safeguards and
19 protections. Why? Because if that data was
20 compromised in anyway, it could affect the safety of
21 the individuals or the officers working on that
22 investigation. Members of the public and indeed the
23 people themselves under investigation who may or may
24 not have engaged in criminal activity. This very
25 strict access to the various databases that we have

2 within the department and it's confined to within the
3 department with different levels of approval. So, we
4 have—we're confident that we have a very secure
5 protection around the data and information that we
6 lawfully collect in this part of various
7 investigative activities. We maintain by state laws,
8 as you know, quite extensive information about sex
9 offenders. It's a statewide form, the Domestic
10 Incident Reports. I think we took about 200,000 of
11 them in 2016. All of that is very sensitive
12 information, and we guard it very carefully for the
13 privacy interests of the victims and for the
14 protection of the public.

15 CHAIRPERSON GIBSON: Okay, and my final
16 question before I turn it over to Council Member
17 Garodnick is to get a commitment from the department
18 that you're willing to work with us on having this
19 further conversation with us on this particular bill,
20 but in general on the level of information that
21 you're willing to share with us that would serve to
22 achieve both public safety as we have been doing, and
23 also making sure that we protect the privacy of New
24 Yorkers. I think in light of—of all that has
25 happened from 9/11 and many communities particularly

2 in vulnerable communities in my district across the
3 city of New York, New Yorkers just want to be
4 reassured that they're not under constant
5 surveillance throughout the city because of what they
6 look like, their religion, where they worship, et
7 cetera, and so to us, you know, this is an approach
8 that we're taking to have a further conversation to
9 stimulate a dialogue because there's a lot of
10 information that we believe that we should receive
11 as a partner with you. Not law enforcement, but
12 legislators in the City Council that has been working
13 with this department for the past four years. So,
14 I'm hoping that we can get that commitment to work
15 with you on finding common ground, and getting real
16 specific details. The commissioner said surveillance
17 technology is too broadly defined. Well, let's
18 specifically define it. So that we can outline
19 exactly what the department can and is willing to
20 share that we all believe is reasonable, practical
21 and—and valid.

22 DEPUTY COMMISSIONER MILLER: I think what
23 the NYPD has demonstrated over almost the last four
24 years now is a very open, willingness to work with
25 this Council, Commissioner Bratton, Commissioner

2 O'Neill and Mayor de Blasio. Through your leadership
3 and the Speaker's leadership we've worked through a
4 number of proposals together that are now law. Just
5 yesterday, officers had a new tool that you gave them
6 that were the months of negotiations and discussion
7 together. They now have the ability to issue a civil
8 summons for certain violations in addition to a
9 criminal summons. So, we are always willing, and we
10 are here today to engage in the dialogue. As Council
11 Garod—Council Member Garodnick is well aware, when he
12 first introduced this bill, we had him over to police
13 headquarters for an extensive multi-hour briefing at
14 high level about the types of technologies we use,
15 how we use them, when we use them, how we don't use
16 them, when we don't use them, when we get a court
17 order, and our concerns about this bill. We're
18 willing to engage in that dialogue with you. Some of
19 it is a dialogue frankly that probably should take
20 place in a closed door setting so that we can be a
21 bit more granular and some of the concerns of
22 disclosing the operational capabilities of
23 technologies. But we most certainly are willing to
24 have that dialogue with the Council in an appropriate
25 way to try to come to a bill that accomplishes what

2 you want, but doesn't accomplish what you don't want,
3 which is a road map for terrorists and criminals to
4 avoid lawful investigative techniques. I think we
5 both agree that no one wants that.

6 CHAIRPERSON GIBSON: Okay. Thank you
7 very much, and we've been joined by Council Member
8 Rafael Espinal, and now we'll have Council Member
9 Garodnick followed by Council Member Lancman. Thank
10 you.

11 COUNCIL MEMBER GARODNICK: Thank you very
12 much Madam Chair. I—I will note that it has been a
13 little difficult in this context to—to engage
14 substantively with the Police Department on this
15 bill. We did have a very productive initial meeting.
16 I think it was even before we had even introduced the
17 bill, and intentionally so because we know that there
18 are concerns here. It is my intention, and always
19 has been to strike the right balance between the very
20 deep and serious concerns that have been articulated
21 by the Police Department, and the need to protect
22 privacy and sensitive information for innocent New
23 Yorkers. We have repeatedly asked for feedback on
24 the draft of the bill that sits before us today, and
25 it is not until today that we're hearing particular

2 questions about definitions of surveillance
3 technology, the impact on sex offenders, gun
4 offenders. All things that, of course we would have
5 been willing even before today to have a change in
6 the bill, to be able to accommodate legitimate
7 concerns from the Police Department. So, I'm very
8 pleased that there is a willingness what the Deputy
9 Commissioner called a logical discussion on this. We
10 appreciate that. I certainly have always been
11 willing to have that, and I certainly hope that you
12 have perceived that because we—we certainly have
13 tried to—to have these conversations. So, let me
14 just go to some of the substantive issues FYI. (sic)
15 The—the policy that is in place for the License Plate
16 Readers, that's really a policy that's in place for
17 the—for the Domain Awareness System. Is that—is that
18 accurate?

19 DEPUTY COMMISSIONER MILLER: Yes.

20 COUNCIL MEMBER GARODNICK: Okay, and that
21 system went into effect in 2009 as I understand it.
22 Is that right?

23 DEPUTY COMMISSIONER MILLER: I believe
24 that's correct.

2 COUNCIL MEMBER GARODNICK: Has the
3 policy—has the—has the system, the Domain Awareness
4 System changed at all in terms of its sophistication
5 or its ability to assess out problems? Has it
6 changed at all since 2009?

7 DEPUTY COMMISSIONER BYRNE: I would have
8 to do a granular examination to answer that. I did
9 review the description of the system before
10 testifying here today, and the privacy policies of
11 the system, and it was largely reflect—reflective of
12 the system as I understand it and accurate, but I
13 would have to—I would have to go back and say since
14 the birth of the system, outside of additional data,
15 the data that's collected over time, what
16 capabilities have changed? Among the capabilities
17 that would have changed is the system is available to
18 more members of the Police Department, and used more
19 effectively in fighting crime everyday because its
20 success stories are piling up faster.

21 DEPUTY COMMISSIONER BYRNE: Just to
22 clarify. One thing that has changed is the
23 accessibility to the DAS system now that all, more
24 than 36,000 of our uniformed officers have Smart
25 Phones they have the ability, and I don't understand

2 the logistics of it to access info off the DAS system
3 through their Smart Phones. That doesn't change the
4 policy of what we record, but it gives them more
5 instant access as they're making snap judgments on
6 the street during incidents and investigations.

7 COUNCIL MEMBER GARODNICK: So, I think
8 it's—it's a great example. Has the—has the privacy
9 policy that was put in place back 2009 been amended
10 in anyway between 2009 and 2017?

11 DEPUTY COMMISSIONER MILLER: I don't now
12 the answer to that, but I do know that having
13 reviewed it, it accurately—it accurately reflects the
14 capabilities of the system, and the privacy—the
15 privacy considerations that are built into it, and
16 published on the website. So, if the—if it--

17 COUNCIL MEMBER GARODNICK: [interposing]
18 Does it address—does it address those new components
19 that Mr. Byrne cited about, you know, 30,000 plus
20 officer now being able to access information on Smart
21 Phones. Does it—does it incorporate the privacy
22 concerns that would be related to—to that information
23 on Smart Phones ?

24 DEPUTY COMMISSIONER MILLER: It doesn't
25 change the principles of the system. The system was

2 always built with the idea that any of our 36,000
3 police officer or authorized civilian employees would
4 be able to access it. The idea that they now have
5 more ability to access it during critical situations
6 in the field is an improvement in the system, but not
7 a change to the privacy considerations as I see it.

8 DEPUTY COMMISSIONER BYRNE: I think as we
9 consider our discussions with you, we should have a
10 more specific discussion about the privacy-privacy
11 interests and policy around DAS. I recall that when
12 I began in this position almost three years ago, I
13 did review that policy very carefully because it was
14 brought to my attention that there are retention
15 periods after which information collected through the
16 DAS system needs to be destroyed, and I do recall
17 that there can only be exceptions to that when
18 someone called the Deputy Commissioner for Legal
19 Matters approves that exception. I have not had a
20 single request for an exception to that policy in the
21 almost three years I've been here.

22 COUNCIL MEMBER GARODNICK: [interposing]

23 I-I-

24

25

2 DEPUTY COMMISSIONER BYRNE: [interposing]

3 Let's--let's have a specific discussion about the
4 policy--

5 COUNCIL MEMBER GARODNICK: [interposing]

6 Absolutely.

7 DEPUTY COMMISSIONER BYRNE: --and share
8 with you what it is.

9 COUNCIL MEMBER GARODNICK: Let me be
10 very clear. I think that it is--it's an extraordinary
11 technological advancement that police officers have
12 the ability to access this, but I also think that it
13 does raise questions about the policy that's in place
14 and whether it should be updated to accommodate the
15 fact that so many more people now have access to
16 information about all of the rest of us as we are
17 walking down the street, whether we're standing in
18 front of Goldman Sachs or going to have a slice of
19 pizza or whatever we're going to do, this is
20 information that's out there that's being collected,
21 and New Yorkers deserve to have some security in
22 knowing that the policies reflect what is actually
23 happening. Let's talk about the other technologies,
24 which I think--which from your testimony I understand
25 you are much less comfortable in--in articulating a

2 public policy for things like and I'm not really
3 asking about stingrays and back scatter specifically,
4 but I do want to know if the Police Department does
5 have internally its own privacy policies as it
6 relates to information that is captured when using
7 these or any surveillance technology that you might
8 employ?

9 DEPUTY COMMISSIONER BYRNE: I think there
10 are two parts to your question. When and how can the
11 different technologies be used, and if they are used,
12 how can the information obtained by the use of those
13 technologies be used? For the first part, again
14 speaking generally, when we're talking about looking
15 at investigating, intercepting things that are
16 happening in private whether it's a legitimate Fourth
17 Amendment privacy interest that all is used pursuant
18 to court order and there are internal guidelines
19 about how and when we use that, and then generally
20 when we obtain the information from that, it can only
21 be used for internal investigative purposes unless a
22 subsequent criminal prosecution ensues in which case
23 the information obtained during that investigation by
24 court order or not court order is turned over to the

2 defendant and her attorney or his attorney for
3 purposes of defending a case against them.

4 COUNCIL MEMBER GARODNICK: So, it sounds
5 like the Police Department does have a policy as it
6 relates to--

7 DEPUTY COMMISSIONER BYRNE: [interposing]
8 It's more than one policy, but yes, a collection of
9 policies.

10 COUNCIL MEMBER GARODNICK: Okay, and does
11 the-the Police Department use stingrays without
12 warrants ever?

13 DEPUTY COMMISSIONER BYRNE: What-I'm not
14 going to talk about the specific Cell-Site Simulator
15 Technology we may use. When we use Cell-Site
16 Simulator Technology we always do it pursuant to a
17 court order supported by probable cause with one or
18 two circumstances involving exigent circumstances.
19 If we have a recent kidnapping or a missing child,
20 and we have the phone, we may go up on the Cell-Site
21 Simulator Technology right away, and subsequently and
22 I mean with 24 or 48 hours apply for the court order,
23 but absent that kind of exigency, we only use Cell-
24 Site Simulator Technology in court ordered supported
25 by probable cause. I want to be very clear here

2 because we work with five district attorneys and two
3 U.S. attorneys in the five boroughs. Some of the—and
4 Cell-Site Simulator Technology as we use it is really
5 a pen register on a cell phone. In the '80s and '90s
6 when I was the federal prosecutor prosecuting
7 organized crime cases, we had pen registers on land
8 lines, and it simply told us what number was calling
9 out and what number was calling. We did that
10 pursuant to a court order not based on probable
11 cause, and then we looked at the patterns of the
12 numbers. Cell-Site Simulator Technology allows to do
13 that on a cell phone, and it gives us one additional
14 piece of information, which we had for land lines.
15 It gives us the location of the cell phone. That's
16 what we use it for. There is Cell-Site Simulator
17 Technology that would allow you to intercept the
18 content of the communications. We don't use that at
19 the NYPD. So, we do it pursuant to court order. In
20 some counties, the district attorney wants to call it
21 a search warrant. In other counties they want to
22 call it a court order supported by probable cause.
23 It's the same thing.

24 COUNCIL MEMBER GARODNICK: Can—can you
25 capture information that is not related to the phone

2 for which you have a warrant while you are capturing
3 information that you're actually looking for?

4 DEPUTY COMMISSIONER BYRNE: I'm sorry.
5 I'm not sure I understand the question.

6 COUNCIL MEMBER GARODNICK: Let's say I'm
7 walking by right next to the person who is the target
8 of your investigation.

9 DEPUTY COMMISSIONER BYRNE: It-it would
10 not tell us anything about you.

11 COUNCIL MEMBER GARODNICK: What-what does
12 it tell you about?

13 DEPUTY COMMISSIONER BYRNE: It tells us
14 where the cell phone is located.

15 COUNCIL MEMBER GARODNICK: Does it if my
16 cell phone is located there?

17 DEPUTY COMMISSIONER BYRNE: Only if you
18 call the person or the person calls you.

19 COUNCIL MEMBER GARODNICK: Okay, so
20 proximity to the-to the cell site locator does not do
21 anything if you are not the target?

22 DEPUTY COMMISSIONER BYRNE: The-the-the-
23 the order and the signal is focused on the specified
24 cell phone and the investigation for which there is
25 probable cause to track it.

2 COUNCIL MEMBER GARODNICK: Okay, I mean I
3 think that this is--this--this colloquially is an
4 important example of what we are trying to share with
5 the public, which is okay, this is not a nefarious
6 use of new surveillance technology. This is an
7 important use of surveillance technology that may
8 have certain guardrails in place already almost
9 always with court supervision.

10 DEPUTY COMMISSIONER BYRNE: Right.

11 COUNCIL MEMBER GARODNICK: That is not
12 something that the Police Department should be afraid
13 to say or share. I don't think that that provides a
14 blueprint for anyone. The notion that we are
15 respecting Fourth Amendment rights, and that we
16 actually are not taking information when it involves
17 individual telephone calls without court order. So,
18 I--I think that, you know, this is--this is my point
19 with the bill. So, I appreciate that, and I think
20 that's--that's important what you just said. Are
21 there surveillance--we--we read a lot about
22 surveillance technologies. You know, the--the various
23 things that may or may not be used. I--I know that--
24 I'm going to assume that you're not going to want to
25 share today if there is surveillance technology,

2 which is being operated by the PD that is not known
3 to the public. So, I—I just will ask this: Who
4 outside of the PD is aware of whatever that is?

5 DEPUTY COMMISSIONER BYRNE: So, there are
6 a couple of issues there, and I wanted to comeback
7 because I think Chairperson Gibson said that there'
8 no oversight of our use of these various
9 technologies. I think there's quite a bit of
10 oversight. We've talked about the oversight that
11 exists when we're getting a court order. To your
12 question: Who's aware of technologies that we have?
13 Obviously, the company or other law enforcement
14 agency that has supplied us with the technology knows
15 that we have it, and it's an important point to note
16 that many of these technologies because they're only
17 effective if bad people don't know how they work, and
18 how to defeat it, are given to us pursuant to very
19 strict non-disclosure agreements. If we had to
20 disclose the operational capabilities of some of
21 these technologies, we might not be able to procure
22 it. We also have oversight, and this is the bill you
23 previously approved, and that this department has
24 embraced certainly under Commissioner Bratton and
25 Commissioner O'Neill, which is the Office of

2 Inspector General, which resides in the Department of
3 Investigation. We have a very robust oversight
4 system at the IG. We've worked very well with the
5 Inspector General. There have been times where we
6 have disagreed with their recommendations, and they
7 have disagreed with some of our policies. But as a
8 working relationship, we have welcomed that
9 independent oversight. In the bill that you created,
10 imposing this oversight on the department, which is
11 why I don't think this provision is necessary in the
12 POST Act. You've already done this. It specifically
13 says that where there are issues about sensitive
14 information, confidential information, the IG and
15 NYPD and if necessary the Mayor will resolve the
16 manner in which the IG gets that information, and
17 conducts their important independent oversight
18 function. So, you have a mechanism in place to have
19 some independent oversight. More recently, and
20 Commissioner Miller alluded to this in his testimony,
21 we have added another layer of independent oversight,
22 which is any of our investigations that are covered
23 by Revised Handschu Guidelines. We now have an
24 independent civilian representative. His credentials
25 are too long to recite here, but a former U.S.

2 attorney, a former federal judge appointed by
3 Democratic and Republic presidents, a former board
4 members of the Brennan Center who sits in and sees
5 every Handschu investigation that we do, every
6 investigative technique that we're using, and he's
7 there to provide some independent confidence to the
8 public that what we're doing, we're doing lawfully
9 and properly, and by the way, if we're not, he's
10 going to go to the judge and report that. So, we
11 have those two levels of oversight in place in
12 addition to the daily court supervision.

13 COUNCIL MEMBER GARODNICK: Is there any-
14 the-the non-disclosure agreements that you have with
15 the companies from which you procure these various
16 technologies, do they-do they preclude the-the Mayor
17 from being able to evaluate your use of that
18 technology?

19 DEPUTY COMMISSIONER BYRNE: Each-each of
20 the non-disclosure agreements, and I've reviewed some
21 personally, but not all of them had different terms.
22 Obviously they would allow the Police Department to
23 know about it because we're procuring it. I think we
24 would take the position that since the Police
25 Commissioner and all of us serve at the pleasure of

2 the Mayor, the Mayor for this purpose is part of the
3 Police Department and not something separate, but I'd
4 have to look at them--

5 COUNCIL MEMBER GARODNICK: [interposing]
6 Well, but I-I guess really-really what I'm asking is
7 if-if the Mayor were to want to conduct some level of
8 oversight as to how a technology is being use, might
9 he be barred by a nondisclosure agreement--

10 DEPUTY COMMISSIONER BYRNE: [interposing]
11 Right.

12 COUNCIL MEMBER GARODNICK: --between the
13 Police Department and the-the company from which
14 you've procured the technology?

15 DEPUTY COMMISSIONER BYRNE: First of all,
16 the Mayor has been very supportive of the Police
17 Department, and very responsive and watching and
18 talking with us about what we're doing, but he has
19 not micromanaged any investigation or any
20 investigative technique. If he has questions for the
21 Police Commissioner, we will find a way to answer
22 those questions without violating any non-disclosure
23 agreement in appropriate private settings so that
24 we're not compromising the ability to use those
25 technologies lawfully.

2 COUNCIL MEMBER GARODNICK: How about—how
3 about a member of the Council, let's say the Public
4 Safety Chair of the City Council?

5 DEPUTY COMMISSIONER BYRNE: I think what
6 I've indicated, and again subject to reviewing the
7 particular agreements is we would be very open to a
8 broader closed door briefing along the lines of what
9 we engaged in with you for the Council so that we can
10 demystify for you a bit what we do and don't do, what
11 we use and we don't use.

12 COUNCIL MEMBER GARODNICK: I—I would just
13 say, and I appreciate that, but respectfully, it's
14 not only about the—the—the comfort of the Council,
15 right. There—there are New Yorkers out there who
16 appropriately question what level of surveillance is
17 being done in their name and with their tax dollars,
18 and they deserve to know, and I—I think frankly for a
19 lot of the stuff, you do, in fact, have policies in
20 place, that you have the policies, that you're
21 following the policies, and that there are perhaps
22 fewer things to be concerned about than people might
23 be concerned about in the absence of knowing any of
24 these things?

2 DEPUTY COMMISSIONER BYRNE: I think all
3 New Yorkers and indeed all people who visit New York
4 including the 60 million tourists who came here in
5 2016, the over one million students attending our 145
6 institutions of higher learning beyond high school,
7 the nearly six million people a day who ride the
8 subway on a business day, and the millions of people
9 who commute into the city have a right to know that
10 whatever their Police Department is doing whether it
11 involves technology or not, is being done lawfully
12 and pursuant to policy and respectfully. Where the
13 line stops is I don't think they have the right to
14 know how a particular surveillance technology can be
15 used, what its operational capabilities are and how
16 its operational capabilities can be defeated. That's
17 where we would draw the line.

18 COUNCIL MEMBER GARODNICK: I think, look.
19 I-I understand that point, and I think that there is
20 a line. I certainly agree there is a line. But just
21 talk for a second about the Department of Justice's
22 policy on Cell-Site Simulator Technology. I don't
23 know if you've had a chance to-to--

24 DEPUTY COMMISSIONER BYRNE: I'm generally
25 familiar with it. With the Department of Justice, as

2 I said, I was federal criminal prosecutor in the '80s
3 and '90s when we had land lines. It was before Vice
4 President Al Gore had invented the Internet, and we
5 used pen registers to get information off of those
6 land lines and then we used wire taps on those land
7 lines. By the way, to the point of adapting when the
8 Mafia had gone through enough--and other organized
9 crime groups had gone through enough cases that they
10 realized we could wire tap phones. What did they do?
11 They started having their conversations in their
12 cars. When they realized we could wire tap cars,
13 they moved into social clubs. When they realized we
14 could put bugs in social clubs, they did long walks
15 on crowded streets where we couldn't intercept their
16 conversations. So, criminals and more recently
17 terrorists have constantly been adapting their
18 tactics in response to legitimate law-lawful law
19 enforcement efforts.

20 COUNCIL MEMBER GARODNICK: Right, okay.

21 So just to the--to the point about this policy--

22 DEPUTY COMMISSIONER BYRNE: [interposing]

23 I'm sorry. So, to answer your question. So the
24 Department of Justice used to use Cell-Site Simulator
25 Technology just based on the equivalent of a pen

2 register order. As a result of losing the case, I
3 believe in Texas, but I'd have to check that. They
4 instituted a policy that they would only use Cell-
5 Site Simulator Technology on a court order based on
6 probable cause. It's the same policy we've been
7 following.

8 COUNCIL MEMBER GARODNICK: Terrific, and
9 I think that actually says a lot. I mean this policy
10 talks about the basic uses, how they function, what
11 they do and what they do not obtain--

12 DEPUTY COMMISSIONER BYRNE: [interposing]
13 Right.

14 COUNCIL MEMBER GARODNICK: --management
15 controls and accountability, legal process, court
16 orders, applications for the use of the Cell-Site
17 Simulators, data collection disposal, training and
18 coordination and ongoing management.

19 DEPUTY COMMISSIONER BYRNE: [interposing]
20 And the--

21 COUNCIL MEMBER GARODNICK: [interposing]
22 That's what the Department of Justice's policy does,
23 and says, and I don't think it's entirely dissimilar
24 from the way--and as I understand it the way the NYPD
25 uses Cell-Site Simulator Technology, and what--but

2 what I don't understand is why is it so risky for the
3 NYPD to put out a policy like this, and not so for
4 the Department of Justice and the federal government?

5 DEPUTY COMMISSIONER BYRNE: I think
6 putting out a policy on when and how we use these
7 things is something we can have a dialogue with you
8 about. Again, how the actual technology operates,
9 how it does its job, what the specifics of it are. I
10 don't think that's appropriate to disclose publicly.
11 We can have a dialogue with you about the policy.
12 There's another layer of confidentiality that's
13 imposed on both the Department of Justice and the
14 NYPD in many cases, which is often when you're using
15 these more sophisticated technologies you're doing it
16 as part of a longer term investigation with the
17 federal prosecutor or with an ADA and with a grand
18 jury in power, and very strict grand jury secrecy
19 requirements about not releasing publicly information
20 obtained broadly during the grand jury process. So,
21 that imposes an additional layer of confidentiality
22 on the NYPD and the federal law enforcement agency.

23 COUNCIL MEMBER GARODNICK: Something,
24 which could easily be disclosed as part of a policy.
25 We cannot disclose when subject to court order, grand

2 jury investigation, et cetera. As a matter of fact I
3 am--

4 DEPUTY COMMISSIONER BYRNE: [interposing]
5 We can work with you on that.

6 COUNCIL MEMBER GARODNICK: --I'm being a
7 little greedy with the time so I'm going to--I'm going
8 to yield the microphone, but--but I look forward to
9 having this continued conversation because I do think
10 that there is an opportunity here, and I do think
11 that there is a line to be drawn. In fact, we've
12 been--we've been trying to draw the line properly.
13 We--we want to work with the Police Department. We
14 respect what you do, and--and hope that we're able to
15 get this bill into the right place. So, thank you,
16 Madam Chair.

17 CHAIRPERSON GIBSON: Thank you, Council
18 Member Garodnick. Next, we'll have Council Member
19 Lancman followed by Council Member James Vacca.
20 Thanks. [background comments]

21 COUNCIL MEMBER LANCMAN: Good morning.
22 So, I'm sympathetic to the concerns that you have
23 about reveal information to the bad guys, which would
24 in some way inhibit your ability to keep us safe, but
25 I--but I do have to say that listening to the

2 testimony and—and the exchanges, I—I think there's a
3 bit of you're not getting it in terms of what is
4 trying to be done with this—with this bill. Military
5 grade X-ray vans, Cell-Site Simulators, License Plate
6 Readers, sonar systems, thermal energy and cameras.
7 These are extraordinary—extraordinarily powerful
8 investigative and intelligence gathering tools, and I
9 am glad that you have them because they are there to
10 keep us safe. But, missing from the philosophy that
11 you outlined for us is a due concern for the—the
12 civil rights and privacy interests of New Yorkers
13 more broadly than just the very, very narrow limits
14 imposed by the Constitution or by courts. The
15 philosophy that you laid out, just to quote from your
16 testimony, I think this is from Mr. Miller's
17 testimony. The philosophy behind—these are some of
18 the tools we're using to keep pace with the evolving
19 threat of terrorism. The philosophy behind them is
20 simple, we have to develop the best intelligence
21 available, expand our partnerships, and take
22 protective measure to defeat whatever our adversaries
23 might be planning next. What I'm not hearing there,
24 and I understand that's just two sentences from the
25 testimony that you provided, but what I'm not hearing

2 there is limiting the intrusion into New Yorkers'
3 privacy to the extent possible and consistent with
4 legitimate law enforcement purposes. That balance
5 between privacy and security is something that I'm
6 sure is part of the department's consideration. When
7 you say that transparency is—is important and—and the
8 department is committed to maintaining the
9 appropriate balance between reasonable transparency
10 and still having the effective tools and technologies
11 needed to protect our city, I—I believe that you
12 believe that. But, ultimately, do you agree that it
13 is the public and their elected representatives who
14 decide the appropriate balance between privacy and
15 security?

16 DEPUTY COMMISSIONER MILLER: I believe
17 that there is a false premise that is a snowball that
18 that's been rolling down the hill, and that is the
19 premise that there is some broad based overarching,
20 undisclosed surveillance of large swaths of the
21 public or neighborhoods or groups or cultures that
22 goes on outside of documented, authorized
23 investigations, that are based on the probability or
24 possibility of criminal activity or terrorism. That
25 is simply not the case, but there is a habit now,

2 there is a trend of calling documented authorized
3 investigations spying, police spying. There is a
4 habit. There is a trend of calling censors or whether
5 they're private security cameras, but thing that we
6 can see right in front of us and pass under everyday
7 calling that surveillance when there's nobody
8 actually watching those cameras, but you can go back
9 to them if there—if there's an incident that has
10 occurred or some reason, and that has all balled
11 up into some kind of paranoia. We operate under
12 strict rules. The largest system concerned here is
13 one that the NYPD proactively disclosed before it
14 was launched, built to the code of the privacy policy
15 that it disclosed, and operates under that policy
16 today. The problem with this bill, and I don't want
17 to sound like a broken record, is not the broader
18 discussions whether to disclose guiding policies, and
19 the use of certain techniques or broader policies on
20 systems, it is that the bill makes no distinction,
21 has no carve-out for redaction, has no exception for
22 sensitive investigative techniques or equipment that
23 would endanger lives. It is simply to disclose
24 everything, every tool, every footprint—

2 COUNCIL MEMBER LANCMAN: [interposing]

3 Well, I'm-I'm glad--

4 DEPUTY COMMISSIONER MILLER: --that you
5 have been involved with the word surveillance.

6 COUNCIL MEMBER LANCMAN: [interposing]

7 I'm glad this year, as my colleague Council Member
8 Garodnick said, and he is the-the author of this
9 bill, I'm glad to hear for the first time that the
10 department is willing to roll up its sleeves and get
11 into the nitty-gritty of the language of the bill,
12 and try to address some of the legitimate concerns
13 that you have. I would make the observation from-in
14 response to-your response to my question that the
15 department has repeatedly over the years pushed the
16 limits of what it can do in terms of intelligence
17 gathering and-and surveillance, and has had to--
18 There's a reason that there's the Handschu Agreement.
19 It is the result of a lawsuit that was brought many,
20 many years ago, and over time on numerous occasions
21 has had to be modified and-and-and expanded. The-the
22 other thing in terms of your concern about the
23 misperceptions that the public has about us living in
24 a surveillance state. My term, my characterization
25 of your term-of your answer is the more that we can

2 inform the public in a responsible way about that
3 surveillance is going on, the less paranoia—your
4 term—will exist, but I have to get back to the
5 question that I asked you because I need to establish
6 a baseline. Do you agree that the balance between
7 security and privacy, the limits of surveillance
8 should be ultimately decided not by the Police
9 Department with all due respect, but by the public
10 and their elected representatives?

11 DEPUTY COMMISSIONER MILLER: The balance
12 when it comes to security versus privacy is decided
13 on a daily basic basis. As Commissioner Byrne
14 described, when you go before a court, and you say,
15 Your Honor, these are the facts as we have them.
16 This is where the investigation may take us, and we
17 would seek the court's permission to go forward, an
18 independent either federally appointed or elected
19 judge reviews that, and as the arbiter that has
20 operated with—within the system for over 200 years,
21 comes to a judgment on behalf of the public as to
22 whether specific tool can be used in the micro sense.
23 In the larger sense, again, not with—not wanting to
24 repeat myself, we have a system like the Domain
25 Awareness System. This system has been laid out

2 broadly and is available for anyone to review on our
3 website.

4 COUNCIL MEMBER LANCMAN: So,
5 respectfully, here's the part that I think you—you
6 don't get. There are tools that are available to
7 you. There are mechanisms, there are devices that
8 are broadly allowable, License Plate Readers for
9 example, which nonetheless and—and a court would not
10 disrupt or block your use of them, but nonetheless,
11 the public might feel that that kind of surveillance,
12 that kind of recordkeeping or whatever it might be
13 might be more than the public is willing to accept in
14 order to achieve whatever security end.

15 DEPUTY COMMISSIONER MILLER: Council
16 Member, it's been in existence since the development
17 of that program, and it's been--

18 COUNCIL MEMBER LANCMAN: [interposing]
19 Well, I-I-I understand, but

20 DEPUTY COMMISSIONER MILLER: --publicly
21 disclosed.

22 COUNCIL MEMBER LANCMAN: --that's just--
23 it's just an example of the fact that there are--

24 DEPUTY COMMISSIONER MILLER:
25 [interposing] It has been publicly disclosed.

2 COUNCIL MEMBER LANCMAN: --tools at your
3 disposal that are much, much, much broader than--than
4 what a court would narrowly block, but which the
5 public might think we don't want that.

6 DEPUTY COMMISSIONER MILLER: I'm sorry
7 and it may be the limits of my own intelligence, but
8 I'm failing to wrap my head around a question about
9 what the public knows or understands about something
10 that we talk about often. In our press conferences
11 and our interviews we talk about the capability of
12 License Plate Readers. We spent a good deal of time
13 as a department after the Boston Marathon Bombing
14 when we were told that the bombing suspects had
15 intended to come to New York and we believed were--

16 COUNCIL MEMBER LANCMAN: [interposing] I
17 get it. So, so--

18 DEPUTY COMMISSIONER MILLER: --but the
19 License Plate Reader system--

20 COUNCIL MEMBER LANCMAN: [interposing]
21 Perhaps the License.

22 DEPUTY COMMISSIONER MILLER: -- didn't
23 detect their entrance into the city.

24

25

2 COUNCIL MEMBER LANCMAN: Okay, I-your-
3 your-I would never challenge your intelligence. So
4 perhaps--

5 DEPUTY COMMISSIONER MILLER:
6 [interposing] One of the reasons I got that word
7 intelligence in my actual job title.

8 COUNCIL MEMBER LANCMAN: Yeah, so-so--

9 DEPUTY COMMISSIONER MILLER: So that it's
10 used with my name in the same sentence.

11 COUNCIL MEMBER LANCMAN: So, so-so
12 perhaps you're being strategically obtuse. Let's-
13 let's say that. [laughter] There are many tools--

14 DEPUTY COMMISSIONER MILLER:
15 [interposing] Get the dictionary.

16 COUNCIL MEMBER LANCMAN: There are many
17 tools that are at your disposal, some of which we
18 know almost nothing about as a matter of policy,
19 which might be, and I assume are, used by the
20 department in strict accordance with the law, but
21 that nonetheless the public and their elected
22 representatives might think even though this is
23 permissible under the law, we would like its use to
24 be narrowed even further because perhaps we are
25 uncomfortable with this level of scrutiny,

2 surveillance, recordkeeping in some governmental
3 database. When I say that that's what you're not
4 getting, that's what I--that's what I mean.

5 DEPUTY COMMISSIONER MILLER: I'd sure
6 like to know what those systems are because if we
7 have those, I don't know about them.

8 COUNCIL MEMBER LANCMAN: Well, if we can
9 pass this bill, I think we'd all get to know what
10 they are, and--and--

11 DEPUTY COMMISSIONER BYRNE: I want to
12 come back to--

13 COUNCIL MEMBER LANCMAN: Yes, sir.

14 DEPUTY COMMISSIONER BYRNE: I want to
15 come back to what I said earlier because I think, and
16 I don't think you intend to do it, but respectfully I
17 don't think you get it. You're misusing the term
18 privacy. Courts have ruled for 200 years under the
19 Constitution and under the State Constitution that
20 what you choose to do in public you have no privacy
21 interest in whether it's driving your horse and buggy
22 to Washington Square, driving your Ford Mustang into
23 New York City, going out lunch time and walk in front
24 of Goldman Sachs there is zero privacy interest in
25 those activities.

2 COUNCIL MEMBER LANCMAN: That's an
3 excellent point . That is the point. Thank you.
4 That is the point. There is a strict legal definition
5 of privacy, which a court will say to an individual
6 sorry, you're in the Midtown Tunnel, you're outside
7 Goldman-Sachs, you're on the street. You have no
8 privacy, but what I am telling you as a
9 representative of 160,000 New Yorkers is that our
10 conception of our privacy interests and--and desires
11 might be broader than that. And, we would like to be
12 able to engage the department in conversation and
13 even direction that to say to you with some of these
14 technologies in some of these circumstance we do not
15 want you to gather intelligence and information to
16 the limit of your Constitutional ability. We might
17 want you to restrict it because maybe we don't want a
18 database out there that's hackable by Wiki Leaks that
19 can, you know, track where Rory Lancman has been all
20 day. That's the thing.

21 DEPUTY COMMISSIONER MILLER: I think we
22 should have that discussion. I think you should hear
23 what we hear when we go around the city. Every
24 tenants association meeting that we meet with in a
25 public housing project wants to know why they can't

2 have a camera in every lobby, and a camera on every
3 elevator. When we talk to victims of transit crime
4 they want to know why there isn't a camera on every
5 part of the subway platform, and every part of the
6 inside of a subway car. When we go and meet with
7 various members of our Muslim community and clergy
8 members, they want to know are we watching people,
9 and have we stopped watching the wrong people because
10 of guidelines because they want to be safe in their
11 houses of worship. So there's a broad diversity of
12 in New York, and there's a broad range of views on
13 that. But, what we hear all the time is that people
14 want us to do things lawfully and respectfully but
15 comprehensively so they don't get shot or killed or
16 die in a terrorist attack.

17 COUNCIL MEMBER LANCMAN: I hear that and
18 I hear other things, and as the elected Council
19 Member, it's my job ultimately to synthesize that,
20 and try to adopt policy for this city. And I thin
21 what this legislation aims at is to get us the
22 information to us and to the public so we can have
23 that intelligent conversation, strike the right
24 balance—a word I've heard a lot this morning—and come
25 up with a policy and policies that are best for this

2 city. But without us having that information, and
3 I'm not saying the exact text of this bill is the
4 final answer, but without us having that information
5 and understanding, we can't do that.

6 DEPUTY COMMISSIONER BYRNE: I think we
7 should continue to have this discussion. I do want
8 to point out because there have been several
9 references to the federal legislation on privacy
10 impact statements that there's a specific exception
11 under federal law that where the disclosure of those
12 statements could compromise ongoing law enforcement
13 efforts, those statements are not to be made public.
14 This bill contains no such provision.

15 COUNCIL MEMBER LANCMAN: And I endorse
16 the—the spirit of that completely. Thank you.

17 CHAIRPERSON GIBSON: Thank you, Council
18 Lancman. Next we'll have Council Member Vacca.

19 COUNCIL MEMBER VACCA: Thank you, Madam
20 Chair. Thank you all. I'm chair of the Committee on
21 Technology so some of my questions will be about
22 technology and contracting. As Councilman Lancman
23 just described, and I'm sure you know, the Council
24 has oversight over city agencies, specifically their
25 budgets. It's our job. Now, as I understand it, the

2 contracts for many of these technologies we're
3 talking about are huge. So, what kind of internal
4 mechanisms are in place to make sure that these
5 contracts with private security and tech companies
6 are held accountable, that they're robust? How much
7 money are we talking about, first of all, and how-
8 what kind of protections do we have built in to make
9 sure that these contracts are—are implemented
10 according to all proper vetting and procedural
11 guidelines of the city?

12 DEPUTY COMMISSIONER BYRNE: So, that's an
13 excellent question because we've—we've left some
14 steps out of the important part of this dialogue, and
15 the Council has a role to play, but there are other
16 elected officials that have a role to play including
17 the Comptroller and the Mayor. So, every contract
18 that the NYPD entered into whether it's for
19 confidential technology or equipment or pens and
20 pencils and legal pads, has to be approved by the
21 Mayor's Office of Contracts and has to be registered
22 by the Comptroller. If the Comptroller does not
23 register the contract, we cannot go forward. Any
24 contracts for the types of technology that we've been
25 talking about here would have to go through that

2 process. Now, the Comptroller has been very vigorous
3 and very responsible he and his staff in the review
4 of these contracts because they recognize the public
5 disclosure of some of the information including the
6 mere fact that we have the capability, could be
7 damaging to public safety in New York City. So, we
8 have an established confidential protocol where the
9 Comptroller can perform his vital and critical
10 oversight function, and decide if he's going to
11 register and approve the contract, but protecting the
12 confidentiality of operational capabilities that are
13 at the heart of our concern about this bill today.
14 And you have the Mayor's Office of Contracts involved
15 with the center (sic) confidentiality provisions as
16 well. The amount of money involved, I would have to
17 get back to you on that. I don't have that
18 information today, but it is a relatively small
19 percentage of our-- I believe this year you gave us
20 a budget of approximately \$5.6 billion. That's an
21 operating budget, and that doesn't include the long-
22 term capital projects like the improvement Rodman's
23 Neck that we plan to make.

24 COUNCIL MEMBER MILLER: I would just like
25 to add to that that the Domain Awareness System,

2 which was built out as a layer of counter-terrorism
3 protective-protection was built almost in total with
4 federal funds from the Department of Homeland
5 Security because of its counter-terrorism protective
6 capabilities and that also goes to pay for a lot of
7 the annual O&M to keep it up and running. The
8 project management there is—we're in the counter-
9 terrorism end of it. The Project Management piece of
10 that in terms of the performance of contractors, and
11 the delivery of services, largely handled by the
12 Internet Technology Bureau of the NYPD and Deputy
13 Commission Tisch.

14 COUNCIL MEMBER VACCA: But, is most of
15 the money we're talking about here federal money, or
16 is this city tax levy money or is it a mix of both?
17 Is it a mixture of both?

18 COUNCIL MEMBER MILLER: So--

19 DEPUTY COMMISSIONER BYRNE: [interposing]
20 We get federal funds—I'll let Commissioner Miller
21 explain. One of the things Commissioner Miller have
22 spent and I have spent along with Commissioner
23 O'Neill a considerable amount of time on in DC over
24 the past few months since the election and indeed
25 even before the election was to preserve the

2 significant cuts in to our UASI funding that first
3 the Obama Administration proposed, and now the Trump
4 Administration has proposed. So, we're fighting very
5 hard to keep those federal funds to operate certain
6 programs that we use. Other programs we use we use
7 city money, but it's a relatively small percentage of
8 our \$5.6 billion budget. As you know, the vast majority
9 of our budget is personnel costs.

10 COUNCIL MEMBER VACCA: Now, you did say
11 that these contracts are a small percentage of your
12 \$5.6 billion budget, but would I be correct in
13 stating that we are talking of several hundred
14 million dollars.

15 DEPUTY COMMISSIONER BYRNE: I can't say
16 that as I sit here today, but I promise to get back
17 to you on that issue. I can't speculate about that.

18 COUNCIL MEMBER VACCA: Okay. When you
19 contract out for services, you have private companies
20 by virtue of contracting out who are doing the work
21 that the city contracts them to do. So, my question
22 is--

23 DEPUTY COMMISSIONER BYRNE: [interposing]
24 That's not correct. When we contract-

2 COUNCIL MEMBER VACCA: [interposing]

3 Okay, correct me.

4 DEPUTY COMMISSIONER BYRNE: When we
5 contract out, we contract in this instance that we're
6 talking about to purchase equipment. Those private
7 companies don't operate that equipment for us. We
8 operate the equipment. We control and contain and
9 protect the information obtained by that equipment.
10 We don't farm that out to private contractors.
11 Policing is done by the NYPD not private contractors.

12 COUNCIL MEMBER VACCA: Okay, then we
13 should not be concerned. That was where my question
14 was headed. We should not be concerned about these
15 private companies having access to information that
16 may be concerned about them having access to?

17 DEPUTY COMMISSIONER BYRNE: The
18 information we obtain through these technologies
19 whether it's done by court order or whether it's done
20 by something that doesn't require a court order or
21 License Plate Readers, remains within the
22 confidential protection of the NYPD and is not shared
23 with outside vendors.

24 COUNCIL MEMBER VACCA: Now, under the
25 agreement there is a revenue aspect of the agreement

2 where the city was going to be collecting 30% of the
3 revenue from future sales of the system.

4 DEPUTY COMMISSIONER BYRNE: This is the
5 Domain Awareness System or DAS?

6 COUNCIL MEMBER VACCA: Yes. So, you-you-
7 so you are aware of it, but have we collected any
8 revenue at this point? Are there expectations and
9 what do you think that revenue will amount to? I'm-
10 I'm interested in the--

11 DEPUTY COMMISSIONER BYRNE: [interposing]
12 Yeah, my-I'll have to get you the numbers. That
13 contract was negotiated before I came on board, but I
14 am largely aware of it. The reason for that
15 provision is that while Microsoft was an essential
16 partner in developing the Domain Awareness System,
17 the NYPD, our Technology and Intelligence and
18 Detective Bureaus made unique contributions to how
19 that system was developed. So it was in effort our
20 intellectual property and ideas that we allowed
21 Microsoft engineers to build for us. Microsoft is
22 then going to be free to go to other departments and
23 agencies around the country and around the world and
24 say we worked with the NYPD to devise these state-of-
25 the art counter-terrorism system for a densely

2 populated urban area and financial district. We felt
3 that because of our unique contribution to that,
4 Microsoft was entitled to their benefit, but we
5 should get our share of the revenue that could go
6 back into the city trust to benefit a variety of
7 programs. That's the history of the contract as I
8 understand it. I don't have specific numbers. I'm
9 happy to get those for you.

10 COUNCIL MEMBER VACCA: But to date have
11 we collected any revenue from that? I know you may
12 not know--

13 DEPUTY COMMISSIONER BYRNE: [interposing]
14 My--my understanding is that we have collected
15 revenue. I just don't know the numbers.

16 COUNCIL MEMBER VACCA: Is this part of
17 your monitoring of these contracts to make sure that
18 the terms of these agreements are lived up to and--

19 DEPUTY COMMISSIONER BYRNE: [interposing]
20 Yes, the--

21 COUNCIL MEMBER VACCA: --that there is
22 accountability--that there is accountability based on
23 what was agreed by the certain vendors?

24 DEPUTY COMMISSIONER BYRNE: Our Office of
25 Management and Budget specifically the contracting

2 section and the Comptroller's Office monitors that
3 there is compliance with all contractual provisions
4 including in those rare instances where we're
5 entitled to revenue that we're getting the revenue.

6 COUNCIL MEMBER VACCA: Lastly, my
7 assumption is that whatever revenue is collected as a
8 result of this would go into the city's general fund?
9 Am I correct in assuming that?

10 DEPUTY COMMISSIONER BYRNE: I'm sure
11 actually.

12 COUNCIL MEMBER MILLER: The construct
13 here is unusual because city agencies particularly
14 the Police Department are rarely in the businesses
15 of-of making a profit. In this case because the DAS
16 system was largely federally funded, the idea of
17 accepting federal funds and then pocketing profits
18 that came from that came to a place where to comport
19 with the rules of Homeland Security funding, the
20 monies that are generated by Microsoft's sales of the
21 system to other jurisdictions are to be put back into
22 the system for operation and maintenance and costs
23 associated with it so that we're not taking federal
24 funds and making what was almost tantamount to
25 commercial profits and putting them into this-the-the

2 general fund. The idea that we are reducing the need
3 to pull on further federal funding by funneling money
4 back into system as its sold to other jurisdictions
5 by the private contractor because of the intellectual
6 property rights that Commissioner Byrne explained.

7 COUNCIL MEMBER VACCA: Okay, I
8 understand. Thank you. Madam Chair.

9 CHAIRPERSON GIBSON: Thank you, Council
10 Member Vacca. I just had a few more questions, and
11 alluding to a little of what the Council Member just
12 talked about, the department gets an amount of
13 funding through Department of Justice, Homeland
14 Security and possibly other federal agencies for the
15 usage of certain technology and equipment. With any
16 of those funds and grants that come to the
17 department, do they come with specific guidelines,
18 rules and regulations that the department has to
19 follow to use this equipment for that money that
20 you're receiving? [pause] Do you want me to clarify?

21 DEPUTY COMMISSIONER MILLER: I wouldn't
22 know. I get the question. I would have to—I would
23 have to research to—to understand it. I mean I don't
24 know what requirements. If you take the Domain
25 Awareness System as an example, the federal

2 government would have attached to that through-
3 through funding it, but I do know that we do have
4 and—and did publish an extensive description of the
5 system, its capabilities and its privacy policies.

6 DEPUTY COMMISSIONER BYRNE: As a general
7 matter on federal funding particularly for counter-
8 terrorism efforts but for law enforcement efforts
9 more generally, the largest chunk of money is the
10 money distributed through the Department of Homeland
11 Security through the UASI program. That is actually
12 a block grant that goes to New York State, and then
13 we in New York City and the NYPD specifically seek
14 our portion of that block grand and we get most, if
15 not all of the money, that New York State gets
16 through that program. The other main program, which
17 is much smaller that we get through DOJ is the Byrne
18 Justice Grant Program. I'm very familiar with that
19 program because it's named for my brother Officer
20 Eddie Byrne. It was created when he was assassinated
21 in 1988 by drug dealers. When we apply for money
22 through the Byrne Grant Program, we're applying for a
23 specific proposal. Please give us \$10 million to do
24 this. Please give us \$5 million to do that. Last
25 year I believe—last year being 2016, we had about \$9

2 or \$9.5 million through the Byrne Justice Grant
3 Program, and I believe we go about \$140 million the
4 UASI funding.

5 DEPUTY COMMISSIONER MILLER: I think \$178
6 million--

7 DEPUTY COMMISSIONER BYRNE: \$178 million.

8 DEPUTY COMMISSIONER MILLER: --through
9 the five different funding streams of UASI funding.

10 CHAIRPERSON GIBSON: Okay. What I'm
11 trying to further understand is if there is any
12 overlap with federal funds, and the usage of some of
13 the technology and surveillance equipment based on
14 what the city contracts out with as well. Further
15 understanding that the federal government any time
16 they give money, it's with conditions, and certain
17 accountability and standards that the department is
18 held to, and at a local level with the level of
19 equipment and services that are provided by the NYPD
20 holding you guys to some sort of level of
21 accountability as well in terms of what you're doing.
22 The federal government with any of the money that
23 they're giving you, they're monitoring what you're
24 doing, and you're held to certain standards, and
25 reporting requirements. And so, you know, trying to

2 look at that model and look at consistency with local
3 money is what the goal of this POST Act, and what
4 we're trying to do. So, that's why I wanted to under
5 with the federal funds what it comes with.

6 DEPUTY COMMISSIONER BYRNE: Yeah, I think
7 we should give you more detail on that as we continue
8 our discussion. I'm aware generally of audits by
9 federal auditors of the UASI funding. The
10 Comptroller after he approves and registers our
11 contracts will often audit those contracts. The
12 specifics of the audit cycle and the requirements I
13 don't have that for you as I sit here today, but
14 we'll get that information for you.

15 CHAIRPERSON GIBSON: Okay.

16 DEPUTY COMMISSIONER MILLER: And our—our
17 performance in those audits over a period stemming
18 from September 11th to date has been exemplary.

19 CHAIRPERSON GIBSON: Okay. With the
20 ongoing technology costs, the contracts that the
21 department enters into with private companies they
22 give you the equipment. The department does the
23 maintenance, the operation of that particular
24 equipment. In terms of the costs for the maintenance
25 and operation, but also I think it was you,

2 Commissioner, that alluded to even Smart Phones and
3 Tablets and the different devices that officer have
4 both patrol and investigators, how is that
5 incorporated into training and costs that are
6 associated with constant changes in technology? How
7 do you monitor that, and are you able to share with
8 us any of those ongoing costs that the department
9 faces?

10 DEPUTY COMMISSIONER MILLER: The
11 transition from the desktop version of the Domain
12 Awareness System to having it available on the Smart
13 Phones, which has been an extraordinary game changer
14 for the capability of police officers was funded in
15 part by the city through tax levy dollars, and in
16 large part by the District Attorney's Office in
17 Manhattan through forfeiture funds seized in-in cases
18 that were to be dedicated back to law enforcement
19 purposes. So that-that covered the costs of the-the
20 Smart Phone program.

21 DEPUTY COMMISSIONER BYRNE: Yeah, another
22 important point here in addition to the federal
23 funding UASI, DHS and the DRJ Byrne Grants, our
24 district attorneys particularly Cy Vance and Judge
25 Brown have been generous-very generous with us

2 funding a whole load of technology initiatives.

3 Recently, Judge Brown gave us almost \$21 million with
4 his forfeiture money to improve vehicles used in
5 Queens North and Queens South. So, that is another
6 source of funding that we get. This is not a repeat
7 funding. It depends on the availability of
8 forfeiture money raised in criminal cases, and how
9 the district attorneys want to distribute that money.

10 CHAIRPERSON GIBSON: Okay, I guess what
11 I-I'm-I'm aware of the work that the DAs have been
12 doing in both Manhattan and Queens and I appreciate
13 that. I guess I was specifically asking about the
14 surveillance technology and how officers are
15 constantly understanding the different technology
16 that they're using for the existing officers, those
17 that are coming out of the Academy. You know, the
18 costs that are--there are costs associated with the
19 training itself. So, that's what I'm trying to
20 understand outside what is the cost? (sic)

21 DEPUTY COMMISSIONER BYRNE: It's more--I
22 think I understand your question better. You're
23 familiar with our TARU unit with the more
24 sophisticated--

25 CHAIRPERSON GIBSON: Yes.

2 DEPUTY COMMISSIONER BYRNE: --

3 technologies, it would be TARU specially trained
4 detectives in the Detective Bureau, specially trained
5 officers in the Intelligence and Counter-Terrorism
6 Bureau who are using those technologies pursuant to
7 court order. As you saw with our body camera
8 procurement process from the start of our pilot, the
9 conclusion that our RFP all sorts of technologies are
10 constantly improving and change-changing. We look
11 from time to time about whether we're using the
12 correct technologies and there needs to upgrade that
13 the officers, the limited number of officers using
14 those-those sophisticated technologies are highly
15 trained.

16 DEPUTY COMMISSIONER MILLER: I'd also
17 like to introduce the distinction in that question
18 because I think it falls back to one of my earlier
19 concerns about the use of the term surveillance or
20 the injection of terms like spying. The average
21 officer and their access to the Smart Phone does not
22 have access to a surveillance tool. What they have
23 access to is data. So, they can look up the police
24 call as it came through the CAD system As they rush
25 to that scene they can touch the number of call back

2 or to the person who called 911 and say this is
3 Officer Jones. I'm on the way. What can you tell me
4 about what's going on there now? They can get to the
5 scene and see the suspect's car and run the license
6 plate, and get the name of who that person may be.
7 These are things that actually happened in the Times
8 Square running down of people from a couple of weeks
9 ago or the Officer Veve incident where they can then
10 figure out okay here's an idea of who we're looking
11 for. They have access to the same data that they
12 would have had access to before this was available on
13 the Smart Phone. They're just able to do it at the
14 scene where they can do something about that data as
15 opposed to driving back to precinct or calling for a
16 specific radio car that had a mobile data-data
17 terminal, which had access to much less. This
18 empower officers to use the information that they
19 have access to as police officers regardless of the
20 vessel it travels through, and to harness that—the
21 power of that information to fight crime, help
22 victims and prevent terrorism.

23 DEPUTY COMMISSIONER BYRNE: And there's
24 another aspect to that tool. Again, just to focus on
25 the Smart Phone for a minute, which I think is a

2 program everybody supports and endorses. Certainly
3 our officers and members of the public do. When I'm
4 getting a 911 job, a radio run to respond to a
5 possible EDB at Apartment 9-A at 36 Clinton Avenue in
6 the Bronx, which happens to be down the block from
7 where I was born, as I'm going to that job, I can
8 call up that location on the Smart Phone, and it will
9 give me the NYPD recent history with that location.
10 Were there any other EDB calls? Were there search
11 warrants? Are there any open arrest warrants for
12 people in there? Have guns been taken out of that
13 location? So, I have much better information about
14 the possible danger that I'm stepping into in that
15 situation and how to address it when I arrive on the
16 scene.

17 CHAIRPERSON GIBSON: Okay, and-and I
18 agree. That's an important tool for officers to use
19 knowing what they're facing as they enter into that
20 apartment or that particular building. I guess I go
21 back to an earlier point that we all keep saying is
22 that there is information that conceivably the NYPD
23 could share with the public on the usage of their
24 public tax dollars, and the goal of our conversation
25 is to find that common balance. Can you tell me the

2 size of the TARU Unit, and SRG and CRC? These are
3 the specialized units that we have. What are the
4 sizes of the units?

5 DEPUTY COMMISSIONER MILLER: CRC has
6 approximately 525 officers assigned to it. The
7 Strategic Response Command has approximately 600. If
8 it doesn't have 600, it is—it is to grow to 600 to
9 cover the five boroughs, and TARU is a much smaller
10 unit that's divided from a—kind of a headquarters
11 base to borough commands because TARU, the Technical
12 Assistance Response Unit performs a number of
13 functions about how they apply technology to exigent
14 circumstances everyday. If there's a hostage
15 situation, TARU is called there to see, you know,
16 what information can we gather to get these hostages
17 released? If there is a kidnapping, TARU will use
18 certain techniques there, and that may be one of
19 those rare exigent circumstances or they may be able
20 to get an emergency authorization, but TARU is a very
21 vital unit.

22 DEPUTY COMMISSIONER BYRNE: TARU has
23 approximately 100 uniformed officers and the other
24 group we shouldn't leave out here with the

2 consolidation of most of those CCB's into Chief
3 Boyce's Detective Bureau. I believe Chief Boyce.

4 CHAIRPERSON GIBSON: [interposing] Right.

5 DEPUTY COMMISSIONER BYRNE: --now has
6 over 5,000 detectives.

7 CHIEF BOYCE: [off mic] It's about 5200
8 of them. [on mic] About 5,200 detectives. All of
9 these detectives are trained uniformly in every
10 application despite their assignment. So, technology
11 plays a big role in that. So, when we do this
12 training, we do it both quarter and both when they
13 come in and at different times in Homicide and Sex
14 Crimes and technology plays a role in that. They're
15 trained specifically in the application in--in getting
16 that--obtaining that warrant for that and also
17 reaching out to other department units to help them.

18 CHAIRPERSON GIBSON: Okay. SRG-2 is in
19 my district in the Bronx, but they respond as needed
20 throughout the city and not just the Bronx, right?
21 Even though we have one in each borough?

22 DEPUTY COMMISSIONER MILLER: SRG is
23 divided up into borough commands, but it is--

24 CHAIRPERSON GIBSON: [interposing] Right.

2 DEPUTY COMMISSIONER MILLER: --designed
3 specifically to have the capability to be a citywide
4 flying squad.

5 CHAIRPERSON GIBSON: Okay.

6 DEPUTY COMMISSIONER MILLER: So, if there
7 was a major event, disturbance--

8 CHAIRPERSON GIBSON: [interposing] It
9 would be deployed?

10 DEPUTY COMMISSIONER MILLER: --or a
11 public event where you needed to gather hundreds of
12 officers without affecting the precinct's ability to
13 respond to calls for service, this is the overarching
14 purpose of SRG. Absent a major event, their main
15 responsibility is to patrol their areas of
16 responsibility to augment the existing patrol force
17 in crime suppression, high profile visibility and so
18 on.

19 CHAIRPERSON GIBSON: Okay, Council Member
20 Garodnick.

21 COUNCIL MEMBER GARODNICK: Thank you very
22 much. It is just a last couple of questions. We
23 appreciate your time. There's obviously a high level
24 of concern about our sanctuary city policies, and how
25 they might be impacted by surveillance, data

2 collected and then ultimately shared with the federal
3 government. In the grants that we get and—and I—I
4 heard the back and forth about the—the use of
5 technology, rules governing the technology, but when
6 it comes to information sharing, how exactly does
7 that work between the NYPD and our federal partners
8 and how can we be certain that it does not actually
9 lead ultimately to immigration enforcement.

10 DEPUTY COMMISSIONER BYRNE: So, let me
11 break it down because there are a number of pieces to
12 your question. With regard to sanctuary cities,
13 again, as Commissioner Miller has said, and I've said
14 before, we're not engaged in a general surveillance
15 program. We're not engaged in a general surveillance
16 program of immigrant communities, of any communities
17 throughout the city. We engage in a variety of
18 surveillances as part of specific investigations.
19 When we share information with other law enforcement
20 agencies, it's done generally on a case-by-case basis
21 where we have an interest or they have an interest or
22 we're working on an investigation together either
23 through a taskforce or some other mechanism. As you
24 are well aware, there is both an executive order and
25 a directive from the Attorney General. So, there's

2 an executive order from the President, to the
3 Secretary of Homeland Security that in awarding funds
4 to local-state and local entities, they will require
5 that local entity to certify that they are in
6 compliance, that basically they're not a sanctuary
7 city, which is not defined. There's no requirement
8 that we provide information back as part of getting
9 funds from DHS. At the DOJ level, Attorney General
10 Sessions has instituted a policy that in order to get
11 money from the Byrne Justice Grant Program the
12 locality applying for the money will have to certify
13 that they are in compliance with certain provisions
14 of federal law, which basically say you can't have a
15 local law that prevents you from sharing information
16 with federal authorities. We don't have such a local
17 law. So we believe that the NYPD is in compliance
18 with that, and that corporation counsel is looking at
19 the issue of whether the city as a whole is in
20 compliance with that provision. But that just says
21 you can't have a law borne that I think doesn't
22 require the disclosure of any actual information.

23 COUNCIL MEMBER GARODNICK: And there is—
24 there is nothing that exists today? There's no
25 allocation for a particular technology or no other

2 system in place that would allow federal sources to,
3 you know, I know there is no general surveillance
4 program, but in the areas in which we are collecting-
5 -

6 DEPUTY COMMISSIONER MILLER: Right.

7 CHAIRPERSON GIBSON: --data in-in, you
8 know on large scales for them to be able to access
9 that?

10 DEPUTY COMMISSIONER BYRNE: Only
11 authorized NYPD personnel can access the range of
12 NYPD database whether information is disclosed
13 because database is on an inquiry by inquiry basis to
14 other law enforcement agencies is something that is
15 reviewed on a case-by-case basis. Again, where
16 there's a lot of misunderstanding I think is when we
17 arrest someone we fingerprint them. When we give
18 someone a desk appearance ticket, we fingerprint
19 them. That fingerprint goes to a database in Albany.
20 That's a state database. We need to send it there
21 because we need to know if there are open warrants
22 from other jurisdictions, and we need to know the
23 criminal history of that individual outside of New
24 York State. Federal agencies do have access to
25 whether people in effect have been fingerprinted, and

2 if ICE or the FBI have flagged someone and we arrest
3 them and send the fingerprints to Albany, they will
4 now know that that person is in the custody of the
5 NYPD, but that's through a state database, not
6 through access to an NYPD database.

7 COUNCIL MEMBER GARODNICK: So, is there a
8 policy within the NYPD about the circumstances in
9 which this information, putting aside the
10 fingerprints for a second because I recognize that's
11 a state database, and we'll—it's state law. But, the
12 question is about internal policies of the PD in
13 determining whether and under what circumstances to
14 share information with other law enforcement
15 agencies. Do those policies exist?

16 DEPUTY COMMISSIONER BYRNE: I don't think
17 it's one policy. I think it's a range of polices.
18 The Detective Bureau has practices. The Intelligence
19 Bureau does. I'll let Chief Boyce and Commissioner
20 Miller speak to that.

21 CHIEF BOYCE: Sure. We have the
22 memorandum—memorandums of understanding with all the
23 federal partners. They are specifically criminal
24 investigations and that's all they are. So, whenever
25 we use our databases, that we have a criminal

2 reservations. It's an understanding that we have
3 with them. They also have their own databases. But
4 just what I said earlier, a very small piece of our
5 investigative units are in federal taskforces and
6 always have criminal investigation only.

7 COUNCIL MEMBER GARODNICK: And how—so in
8 the context of a criminal investigation, and I don't
9 even know what sort of information you're sharing,
10 but let's just—we'll just take a batch of information
11 that the NYPD has collected and has now shared
12 through taskforces or other mechanisms with federal
13 sources. What—what is the basis for our confidence
14 that—that information is not going to lead to
15 immigration enforcement?

16 CHIEF BOYCE: Well, the immigration as I
17 said before it's only criminal. We will not do any
18 other thing outside of a criminal investigation. So,
19 if a federal authority wants our databases, gang
20 databases to see if this person is in a gang there,
21 we will share that because we're in a gang—a gang
22 case. So, I don't, you now, the memorandum says
23 this. I can't tell you what—what authorities we do
24 with other than the criminal case. It is under the
25 supervision or a—of the Southern District of Eastern—

2 Eastern New York. So, that's where we—that's where
3 we are with that.

4 DEPUTY COMMISSIONER BYRNE: Remember, we
5 don't do civil immigration enforcement, and when we
6 talk to crime victims and crime-witnesses to crimes,
7 we don't ask them their immigration status and we
8 don't track that. So, even if ICE or the FBI said
9 you had an encounter with, you know, Larry Byrne, did
10 you have an encounter with Larry Byrne on December
11 20th? We're investigating him for a possible crime,
12 a kidnapping or the criminal federal illegal re-entry
13 into the country. We wouldn't be able to tell you
14 that person's immigration status because we don't
15 track that. At one time we tracked that because we
16 were required to certain federal treaties and laws.
17 When we arrest someone, if they are a citizen of a
18 foreign country, we often have to notify their
19 consulate that we have one of their citizens in
20 custody so the consulate can take action to protect
21 their interests just as if an American citizen was
22 arrested in Paris, the Paris police would notify the
23 U.S. Embassy that we have your citizen in custody on
24 the following charges.

2 COUNCIL MEMBER GARODNICK: But as-as I
3 understand it, and I'll-and I'll let it be, but if we
4 do refer information over to our federal partners on
5 a criminal matter we no longer have the ability to
6 control where that information goes correct? I mean
7 it's now in the hands of federal government. If they
8 want to throw it over to ICE, if they want to throw
9 it over to the Department of Justice, if they want to
10 do whatever they will do with it, they will, right?
11 We-we retain no-no further control over whatever we
12 turn over to them. Is that fair?

13 CHIEF BOYCE: I would say I would ask
14 them that question not me, but when--

15 COUNCIL MEMBER GARODNICK: [interposing]
16 But you know of no control that you have--

17 CHIEF BOYCE: [interposing] I don't know
18 that so--

19 COUNCIL MEMBER GARODNICK: --after you
20 turn it over.

21 CHIEF BOYCE: --it would be conjecture
22 for me to say any more than that what happens in any
23 cases other than the fact that it's a criminal
24 investigation under the auspices of-of the Southern
25 or Eastern District. (sic)

2 DEPUTY COMMISSIONER BYRNE: Just as we've
3 tried to indicate today that our relationships with
4 other local, state and federal law enforcement
5 agencies is very important to everything we do on
6 traditional crime and terrorism. It's equally
7 important to them so they have the same interest to
8 treat responsibly any information we give them as
9 part of the criminal investigation.

10 COUNCIL MEMBER GARODNICK: Okay, I-I
11 think, you know, part of the—one of the elements of
12 this bill obviously is the question about how exactly
13 and under what circumstances sensitive data that's
14 obtained through surveillance is shared with
15 partners, and we recognize that this is routinely
16 done in the context of criminal investigations
17 through the auspices of the Southern or Eastern
18 District or even through the Department of Justice
19 directly, but—the not that we would have a policy or
20 be able to articulate what that policy is recognizing
21 that once it is in the hands of the federal
22 government we've lost our control over any of this
23 data. But if we are collecting it ourselves, we
24 should at least be able to state, I think, what the
25 policies and circumstances are in which we are

2 sharing it, and so I thank you. Thanks for that,
3 Madam Chair.

4 CHAIRPERSON GIBSON: Thank you very much,
5 Council Member and we have two other panels after
6 you. So, we thank you for your presence today. Thank
7 you, Ole. Thank you Commissioner Byrne. Thank you
8 Commissioner Miller and Chief Boyce. A work in
9 progress. We look forward to continuing to have
10 these conversations with you, and I also ask as you
11 leave, I need to make sure you have a staff that
12 remains behind so that they can hear from the
13 advocates and other interested New Yorkers who are
14 here. Okay, thank you very much.

15 DEPUTY COMMISSIONER BYRNE: Thank you.

16 CHAIRPERSON GIBSON: Our next panel is
17 [shushing for quiet]

18 SERGEANT-AT-ARMS: Quiet down, quiet
19 down. [background comments]

20 CHAIRPERSON GIBSON: Thank you. Our next
21 panel for today's hearing is Chad Marlow from ACLU;
22 Rashida Richardson from New York Civil Liberties
23 Union; Wesley Alexis from NYC Privacy; Albert Kahn
24 from Care NY; Michael Price, Brennan Center for
25 Justice; and [background comments, pause] and Muzna

2 Ansari from New York Immigration Coalition. If
3 you're here, please come forward. [pause] Okay.
4 Thank you all for being here. I also want to
5 acknowledge that we've been joined by Council Member
6 Jumaane Williams and you may begin. Make sure your
7 mic is on.

8 MICHAEL PRICE: Good afternoon, Chair
9 Gibson and members of the Public Safety Committee.
10 My name is Michael Price and I serve Counsel in the
11 Liberty and National Security Program at the Brennan
12 Center for Justice. Thank you for holding this
13 hearing and inviting us to testify in support. The
14 Brennan Center commends the Council on its thoughtful
15 approach to balancing the need for democratic
16 oversight, and transparency with the NYPD's
17 legitimate need for operational secrecy. I'd like to
18 focus my remarks on that point today. Although the
19 NYPD may wish not to discuss the surveillance tools
20 they use, a strong local democracy like New York City
21 requires a basic level of information about what its
22 local police are doing and how they're doing it. The
23 POST Act will inform the public and critically
24 members of the City Council about the kinds of
25 information that the NYPD collects and the policies

2 in place for retaining, sharing and protecting it.
3 Such information is essential to effective public
4 oversight, but it is too general to be of use as a
5 tool for those wishing to evade lawful police
6 surveillance. It does not disclose information about
7 how the NYPD uses the technology in connection with
8 specific investigations, where or when it might be
9 used or how someone might defeat it. It also does
10 not make the tools any less effective. Wire taps,
11 for example, remain a potent investigative tool
12 despite widespread knowledge of their existence and
13 very strict rules for their use. The NYPD might
14 enjoy a brief tactical advantage if it were to
15 secretly acquire a new technology that is unknown to
16 the general public, but history shows that the public
17 inevitably finds out and the failure to properly
18 disclose information about surveillance technologies
19 to judges and criminal defendants can jeopardize
20 thousands of investigations as was the case in
21 Maryland and Florida. The goal of the POST Act is to
22 frontload the discussion. To have an informed
23 conversation with policymakers and community
24 stakeholders about the rules of the road before the
25 NYPD develops and deploys a new technology, before

2 there is another alarming headline about police
3 surveillance. This is a common sense idea embraced
4 by law enforcement leaders. For example, the two
5 federal agencies responsible for protecting our
6 domestic national security the Department of Homeland
7 Security and the Department of Justice have published
8 their policies on the use of Stingrays and other
9 surveillance technology that NYPD would keep secret.
10 If these two agencies responsible for our national
11 security can disclose its information publicly, there
12 is no reason why the NYPD cannot do so as well. New
13 Yorkers all want the NYPD to keep us safe, but ne
14 surveillance technologies do not just capture
15 information about the bad guys. They affect the
16 privacy of rights of all New Yorkers especially and
17 disproportionately communities of color. Without
18 some basic information about what these technologies
19 do and how the NYPD is using them, lawmakers and the
20 government, and government watch dogs including the
21 NYPD Inspector General will have a difficult time
22 doing their jobs effectively. Transparency and
23 oversight are essential features of a strong
24 democracy. The Brennan Center strongly supports the

2 POST Act and urges the Council to pass it quickly.

3 Thank you.

4 CHAIRPERSON GIBSON: Thank you very much.

5 You may begin. Thanks.

6 CHAD MARLOW: Madam Chair, Council Member
7 Garodnick and members of the Public Safety Committee.
8 My name is Chad Marlow and I'm an attorney with the
9 American Civil Liberties Union. Today, I'm pleased
10 to offer the ACLU's strong endorsement of Intro 1482,
11 the POST Act. While I gave submitted more detailed
12 written testimony, for purposes of time I will limit
13 my remarks to a single subject: The POST Act's
14 ability to stymie the agenda of President Trump. When
15 Donald Trump ran for president he told the American
16 public he would focus his efforts on identifying and
17 deporting millions of undocumented immigrants, on
18 tracking and surveilling Muslims throughout the
19 country and banning their travel to this country and
20 in promoting even more aggressive policing against
21 communities of color. At least in this regard, our
22 president has been a man of his word. To effectively
23 pursue these policies, which involve targeting
24 millions of people, President Trump needs the help of
25 local law enforcement. Fortunately, the Mayor has

2 assured us the NYPD will not actively assist Trump in
3 pursuing his agenda, and we are grateful for that.

4 But while New York City has posted guards at its
5 front door to prevent Trump from going after these
6 vulnerable communities, the city has left no one
7 guarding its back door. What is that back door? It
8 is providing the Trump Administration with direct or
9 indirect access to NYPD surveillance data in exchange
10 for grants to purchase surveillance technologies.

11 This federal threat is not science fiction. It is
12 science fact. By way of example, in Oakland,
13 California another sanctuary city, the city's Privacy
14 Advisory Commission uncovered evidence that the ICE
15 has been accessing the Oakland Police Department's
16 automatic License Plate Reader Data to go after
17 immigrants. Does the NYPD have such data sharing
18 agreements? You, the members of the City Council
19 have no idea. The public you represent has no idea.
20 The NYPD has kept us in the dark because it has the
21 unchecked authority to make these decisions in
22 secret. The only way to change that practice is to
23 change the law, and that is what the POST Act is all
24 about. If adopted, the POST Act would require the
25 NYPD to provide the Council and the public with

2 specific information about proposed surveillance
3 technology acquisitions and uses including data
4 sharing so we are empowered to raise objections.
5 Through that simple accomplishment, the POST Act
6 would undermine the Trump Administration's ability to
7 secretly use NYPD surveillance technology to target
8 vulnerable communities. You want to know what the
9 resistance looks like? The POST Act is what it looks
10 like. The POST Act provides a real opportunity to
11 make New York City a place where everyone is welcome
12 and everyone is safe. Anti-Trump words are not
13 enough. Action is required and now you have an
14 opportunity for action. The ACLU respectfully
15 requests you support the adoption of the POST Act.

16 CHAIRPERSON GIBSON: Thank you very much.
17 It's a hard act to follow. Wow. [applause] Well,
18 sorry, we don't clap. We just go like this. We just
19 shake. [laughs] Thank you very much. You may begin

20 RASHIDA RICHARDSON: Good afternoon. My
21 name is Rashida Richardson and I'm the Legislative
22 Counsel at the New York Civil Liberties Union. The
23 New York Civil Liberties Union respectfully submits the
24 following testimony in Support of Intro 1482, the
25 POST Act: The NYPD uses numerous forms of powerful,

2 invasive and covert surveillance technologies to
3 police New York City streets everyday. These
4 surveillance technologies can capture vast amounts of
5 information about the places we visit, the people we
6 communicate with, the frequency of those
7 communications, where we are located inside of our
8 homes and our most recent social media post. While
9 surveillance technologies by themselves can pose
10 significant risks to privacy, public health and civil
11 liberties and right, the lack of transparency and
12 oversight regarding how these technologies are
13 acquired and used by the NYPD threatens our
14 democracy. To date, most of what we know regarding
15 NYPD's use of surveillance technologies is based on
16 costly FOIL litigation, investigative journalism and
17 inquires by the criminal defense community. An
18 example that illustrate the problems created by the
19 lack of transparency and oversight regarding the
20 NYPD's acquisition and use of surveillance
21 technologies are x-ray vans. X-ray vans are military
22 grade surveillance equipment, which utilizes x-ray
23 radiation to see inside of cars and buildings. These
24 devices were used to search for roadside bombs in
25 Afghanistan, but are also used on the streets of New

2 York City. The company that manufactures x-ray vans
3 determined that vans expose bystanders to a 40%
4 larger dose of ionizing radiation than that delivered
5 by similar airport scanners. Exposure to ionizing
6 radiation can mutate DNA and increase risk of cancer.
7 In fact, the European Union and US TSA banned the use
8 of this type of radiation technology in airports,
9 citing privacy and health concerns. Additionally, x-
10 ray vans cost around \$800,000 per unit, which can
11 have significant fiscal implications. Until Pro
12 Public had a FOIL lawsuit nearly five years, which
13 revealed some of what we know about x-ray vans, the
14 NYPD has largely refused to disclose any information
15 about how they use x-ray vans on the streets of New
16 York. The NYPD has attempted to keep these devices
17 secret, has run counter to best practices used by
18 other agencies including the Department of Homeland
19 Security, which already revealed the same information
20 being sought by the ProPublica in its FOIL
21 litigation. The NYCLU has been at the forefront of
22 bringing NYPD's use of surveillance technologies into
23 the light for many years. However the public should
24 not have to learn about these technologies through

2 costly litigation, and this is why we need the City
3 Council to pass the POST Act now.

4 CHAIRPERSON GIBSON: Thank you very much.

5 ALBERT KAHN: Good afternoon. My name is
6 Albert Kahn (sic) and I serve as the Legal Director
7 for Care New York, a leading Muslim civil rights
8 group. I speak today in support of the POST Act,
9 which would be an important step forward in
10 strengthening police oversight, promoting public
11 safety, and safeguarding New Yorkers' privacy rights.
12 Today my oral remarks are excerpt of the longer
13 written statement we have submitted into the record.
14 Before I begin, I want to answer clearly and
15 succinctly a question that Rory Lancman asked just a
16 few minutes before to the NYPD: Who makes the
17 decision of how to balance privacy and surveillance?
18 The answer is quite clear. It is the elected
19 representatives of this city, and the people they
20 serve, not the NYPD. Historically, the NYPD has
21 deployed novel and highly invasive technologies in
22 ways that circumvented democratic oversight and
23 accountability, and the POST Act would reform these
24 abuses offering protection to all New Yorkers, but
25 particularly its Muslim communities. One reason why

2 the POST Act is so crucial is that many of the most
3 invasive NYPD programs have never produced a single
4 lead let along stop a terrorist act. Yet, these same
5 tactics and technologies whose rewards are so
6 nebulous have a very clear cost. Although most
7 Muslim New Yorkers continue to unapologetically
8 practice their faith in the face of police
9 harassment, some have stopped attending their places
10 of worship. Those who continue to attend services
11 face frequently insurmountable barriers to building
12 trust with those around them knowing that a friendly
13 co-congregate may secretly be an undercover officer.
14 Other New Yorkers are afraid to practice their faith
15 as they'd wish refraining from wear a beard, a
16 headscarf or other visible signatures of their
17 religion. Moreover, Muslim faith leaders often speak
18 guardedly to their congregations fearful that an out
19 of context statement or even a disfavored dialect
20 might spark an investigation. These anecdotes are
21 not anomalous. According to the Office of the
22 Inspector General for NYPD, over 95% of recent NYPD
23 political and religious investigations targeted
24 Muslim individuals and organizations. The pattern of
25 discriminatory surveillance is completely at odds

2 with the fact that the overwhelming majority of
3 terrorist attackers in the United States are
4 committed by right wing extremists and right
5 supremacists. Let me repeat that face since it's
6 often ignored. Right wing extremists and white
7 supremacist commit the overwhelming majority of
8 terrorists attacks in the United States. That is not
9 a finding from Care New York. That is in groups—in
10 groups ranging from the Anti-Defamation League to the
11 Southern Poverty Law Center to the U.S. General
12 Accountability Office. The novel NYC-PD surveillance
13 practice is governed by the POST Act, and completely
14 invisible to the targets making them much more
15 dangerous to our freedom of speech and religion. The
16 need for oversight is only heightened by the NYPD's
17 clear track record of disregarding those few
18 restrictions on existing surveillance practices.
19 According to the—according to the OIG, over half of
20 NYPD Intelligence investigations continued even after
21 legal authorization expired, and for this reason, I
22 look forward to working with this Council to protect
23 the rights of Muslim-Americans in the months and
24 years to come.

2 CHAIRPERSON GIBSON: Thank you very much.
3 Thank you. You can begin.

4 MUZNA ANSARI: Good afternoon. Thank you
5 Public Safety Chairperson Vanessa Gibson and Council
6 Member Garodnick for allowing the New York
7 Immigration Coalition to testify today on the POST
8 Act. My name Muzna Ansari, and I am the Immigration
9 Policy Manager at the NYIC. The NYIC is an umbrella
10 policy and advocacy organization that represents over
11 150 non-profit members serving immigrants throughout
12 New York State. For the last 30 years, the NYIC has
13 engaged in advocacy at the city, state and federal
14 level to protect immigrant communities. Due to the
15 enforcement implications of surveillance and
16 information sharing, the NYIC strongly supports
17 passage of the POST Act. Thank you to the Council-
18 the Council for introducing this important piece of
19 legislation that will help ensure transparency and
20 increase accountability of the NYPD. Given the
21 Federal Administration's unwavering attack on
22 immigrant communities, it is vital now more than ever
23 that the public be aware of what information the New
24 York City Police Department collects and subsequently
25 shares with federal agencies. It is also critical in

2 this political climate for the public to know exactly
3 which agencies this information is shared with.

4 Given the recent uptick in immigration enforcement,
5 immigrant communities are living in fear right now.

6 In the eyes of undocumented immigrants any
7 interaction with local law enforcement can lead to
8 significant ramifications. There are rampant rumors
9 in the community of enforcement occurring as a result
10 of interaction with agencies like the NYPD.

11 Immigrants are less-less likely to trust law
12 enforcement and far less likely to report crime or
13 cooperate in investigation and prosecution of
14 criminal activity. Given the NYPD's history of
15 surveillance of the Muslim community, there is also a
16 deep distrust among Muslim New Yorkers of local law
17 enforcement. At this critical time, it is vital that
18 the public know what kinds of data the NYPD collects
19 and disseminates and again with whom that information
20 is shared. Currently, the NYPD faces no incentive of
21 city requirement to-[coughs] to without information
22 from federal agencies, as surveillance technologies
23 employed by the NYPD are often funded as we learned
24 today and know from federal agencies. And as
25 surveillance technologies employed by the NYPD are

2 often funded by—specifically by federal grants or
3 private donors. As a result, surveillance
4 information sharing is currently inadequately
5 monitored. For example, New Yorkers do not know if
6 the NYPD shares information even if it is regarding a
7 criminal investigation with ICE, and this information
8 can lead to apprehension and deportation of immigrant
9 New Yorkers. While the city took a significant step
10 in protecting immigrant communities by passing anti-
11 detainer legislation, it must now play this—it must
12 now apply the same level of commitment to ensure
13 transparency regarding information sharing between
14 NYPD and federal agencies. We applaud the POST Act's
15 requirement that the NYPD publicly share details
16 regarding its use of surveillance technology, but we
17 do call on the Council to take this bill one step
18 further. The POST Act should explicitly require the
19 NYPD to disclose which agencies it shares information
20 with. This level of transparency and accountability
21 will bring New York City [bell] closer to being a
22 true sanctuary city, and providing its immigrant
23 communities the protection they deserve. Thank you
24 again to the Council for addressing this important
25 issue and allowing the NYIC to testify today. We

2 look forward to working with you to ensure the
3 privacy and rights of immigrant New Yorkers.

4 CHAIRPERSON GIBSON: Thank you very much.

5 WESLEY ALEXIS: Hello, my name is Wesley
6 Alexis. I am a supporter for the NYC Privacy Board
7 Advocates. We advocate for the creation of a Privacy
8 Guidelines Board to advise city legislators and
9 agencies in the creation of policies that will
10 protect New Yorkers' data from being misused or
11 abused. NYC Privacy Advocates—excuse me—NYC Privacy
12 supporters demand that the city create strong
13 policies and oversight to keep pace with a ton of
14 technologies that have potential to for unintended
15 disclosures or abuse of individuals' data. We feel
16 that the POST Act works towards our vision. The POST
17 Act events the opportunities for New Yorkers to
18 influence how technologies are used in our society.
19 In this way, it allows New Yorkers to proactively
20 limit unintended consequences, and prepares us to
21 handle. The growing power of technologies and how
22 they integrate into our society must be matched by a
23 proportionate responsibility for how they are used.
24 We feel that this must be a multi-lateral discussion
25 and so we do not necessarily take a particular stance

2 on the issues of surveillance. Rather, we invite New
3 Yorkers to have more of a way to discuss and
4 proactively work with that. Thank you.

5 CHAIRPERSON GIBSON: Thank you very much.
6 I appreciate it. We were joined earlier by Council
7 Member Ritchie Torres, and Council Member Jumaane
8 Williams. You know, Council Member Garodnick just
9 stepped out. So, I apologize, but I thank you all
10 for your testimony and also for just supporting the
11 POST Act, and everything that we believe this act is
12 going to do. I thank you for the work that you do in
13 your capacities as well because this is really about
14 achieving that balance that we keep talking about of
15 protecting everyone's civil rights, their privacy,
16 but also making sure that we continue to keep every
17 New Yorker safe. So, I thank you on behalf of
18 Council Member Garodnick and myself, and we look
19 forward to working with you. We are certainly going
20 to need your help as we keep pushing this POST Act.
21 So thank you for your testimony and thank you for
22 coming this afternoon. Thanks. Our next panel is
23 Jerome Greco from the Legal Aid Society; Yung-Mi Lee
24 from Brooklyn Defender Services; CO Chin from
25 Restore the Fourth; Kelly Grace-

2 KELLY PRICE: Price.

3 CHAIRPERSON GIBSON: Oh, Price. Thank
4 you—from Jails Action Coalition; and Towaki Komatsu
5 (sp?) representing himself. [pause] Okay, you can
6 start. You can begin. Thank you everyone for coming
7 today.

8 JEROME GRECO: Thank you. Good
9 afternoon. I'm Jerome Greco a staff attorney at the
10 Digital Forensic Unit at the Legal Aid Society. The
11 Legal Aid Society as a primary public defender in New
12 York City combined with our digital forensic ability
13 gives us a unique position to address many of the
14 NYPD's Technologies. So, thank you for giving us
15 that opportunity to speak on the POST Act. During
16 the testimony of the NYPD's representatives there was
17 a claim that all their technologies—that all their
18 technologies to be used follow constitutional
19 provisions and laws. From 2008 to 2015, the NYPD
20 used a Cell-Site Simulator, commonly referred to as a
21 Stingray device over 1,000 times without once
22 obtaining a warrant. The Legal Aid Society has
23 identified three open cases in which we believe that
24 a Cell-Site Simulator was used and have had the
25 prosecution confirm our—a suspicion—our suspicions in

2 one case. No warrant was obtained in that case, only
3 a pen register order. The statute for Pen Register
4 Orders does not cover Cell-Site Simulators, and the
5 applications submitted to the courts do not mention
6 Cell-Site Simulators and mislead judges about what
7 they are ordering. Pen Registers are defined under
8 CPL 705.00 Subsection 1 as a device which records or
9 decodes electronics or other impulses, which identify
10 the numbers dialed or otherwise transmitted or the
11 telephone line to which such a device is attached.
12 There is nothing in there about location or finding
13 someone's location. Yet—thank you—yet, the NYPD is
14 using it to find people's location, and they are
15 obscuring the fact of what the technology they are
16 using, which prohibits judges from being able to
17 identify and understand what they're sign—signing and
18 also prohibits defense attorneys from knowing what
19 actually was used. It wasn't until very recently
20 that this was known at all, which is why the—the
21 Legal Aid Society had been unable to identify this in
22 the past because of the NYPD's attempts to obscure
23 their use of these things. The technology used by
24 the NYPD that was not discussed so much today is
25 Facial Recognition Technology. Current Facial

2 Recognition Technology has been shown to be more
3 likely to misidentify African-Americans and it is
4 more likely to produce false positive matches of
5 young adults. Mainly in today's societies, clients
6 are young people of color who struggle—who already
7 struggle with the biases of the Criminal Justice
8 System, and do not need an additional bias from a
9 secretive software with limited to no oversight. The
10 Post Act can address program. In regards to the
11 automatic License Plate Readers, the NYPD did not go
12 into much detail about the fact that they also have a
13 private contract with a company called Vigilant
14 Solutions, which in 2004, in the agreement Vigilant
15 Solutions, the company bragged that it had 2.2
16 billion records and was collecting 100 million
17 records per day on License Plate Readers across the
18 country including using private fleets to do so. We
19 know that NYPD also receives some of its License
20 Plate Readers data from other police departments in
21 the area including the New York State Police, Suffolk
22 County Police and New York-New Jersey Port Authority,
23 and there's no indication to us at least that any
24 restrictions about sharing—about how the data is
25 shared back if done at all. The POST Act is

2 necessary and the Legal Aid Society encourages the
3 City Council and the administration to pass it.

4 CHAIRPERSON GIBSON: Thank you very much.

5 C.O. CHIN: We started forces as a
6 national civil liberties organization urging you to
7 adopt the Post Act. We fully endorse the comments—
8 the comments presented by the NYCLU, and we would
9 like to add a few remarks regarding the way in which
10 this legislation would restore the protection
11 embodying the Fourth Amendment of our Constitution.
12 The Fourth Amendment protect U.S. residents from
13 search and seizure with our probable causes. It
14 requires transparency for us emphasizing the role of
15 independent external review before law enforcement
16 conducts search and seizure. When it comes to
17 technology, from Stingray to drone to x-ray vans, the
18 NYPD has tried very hard to hide this technology from
19 any external review from the equipment they acquire
20 to the surveillance they conduct. It is high time
21 for this to change. Passing the POST Act would
22 finally require the NYPD to develop policy for
23 deploying the new technology before its deployment,
24 and it would give you members of the Council a really
25 necessary assessing it for reasonability. We expect

2 this policy will specify whether a warrant will be
3 required and whether incidentally gathered data can
4 be retrained for use in future investigations. It is
5 easy for new surveillance technology to turn into
6 dragnet. The POST Act creates the mechanism for
7 preventing such dragnet, and it creates the
8 responsibility in the most appropriated hand, the
9 City Council. Without democratically elected
10 officials along with the input of the people who
11 attend and testified at public hearings like this
12 one. We care desperately about the Fourth Amendment
13 and see it under increasing-increasing threet-threat.
14 A public review process for surveillance technology
15 we allow the discussion and the debate-and debate
16 informed by the perspective of elected officials, the
17 general public and the technology experts and not
18 just the perspective of law enforcement. That's a
19 balance we sorely need. Thank you very much.

20 CHAIRPERSON GIBSON: Thank you very much.
21 Before you begin, I just want to acknowledge we have
22 the student government here from Dr. Betty Shabazz
23 School PS 298 of Brooklyn. Welcome to City Hall.
24 Thank you so much for coming today. We love to see
25 our students come to see City Hall and the City

2 Council in action. So thank you for joining us at
3 today's hearing. Welcome once again. [background
4 comments, pause] You can begin. Thank you.

5 KELLY GRACE-PRICE: That's why they call
6 me Grace. [laughter] Everything is not graceful in
7 my life. So my name is Kelly Grace-Price and thank
8 you for having this hearing today. I have testified
9 in front of you before Councilwoman Gibson
10 specifically about what happened to me in your
11 district in the 28th Precinct as a domestic violence
12 survivor when I went to that precinct for help if you
13 recall, my abuser was a snitch for Cy Vance in
14 Operation Crewcut. So instead of impugning his
15 credibility, I was turned into Rikers and charged
16 with 324 counts of CPR 240.30, which has now been
17 ruled unconstitutional, in order to shut me up and to
18 keep the credibility of my batterer passing forward
19 proffer to the NYPD that helped him assist in making
20 all those big Operation Crewcut gang busts in the
21 Manhattanville Projects, the 137th Street Gang, the
22 Good Fellows, et cetera. He knew all about these big
23 Crewcut operations. So, they're done on the backs of
24 domestic violence survivors like me, and what happens
25 when we come forward to complain about our treatment

2 by our batterers who are given carte blanche to our
3 operate with impunity and abuse us is we're put on t
4 a do not serve list by the NYPD. Who are the NYPD
5 reps here taking notes for your bosses that were left
6 behind? Is it you in the front? So, we're put on a
7 do not serve list. It's called the Arrest Alert List
8 with a COMPSTAT database. We are put on this list
9 as—and marked as fabricators who are no longer to
10 receive police services. The way we were put on this
11 list is a mystery. There's no oversight. Cy Vance
12 himself in a New York Times Magazine article of
13 December 15, 2014 said that people are put on this
14 list because they are uncooperative witnesses that
15 the Criminal Justice System wants to incapacitate
16 using the Criminal Justice System. Some of them are
17 grand larcenists, some of them are repeat offenders,
18 but we have no idea who gets put on this COMPSTAT
19 arrest list—alert list, and who is denied police
20 services. Now, as a domestic violence survivor, I've
21 moved out of the 28. I now live up in the 34. I
22 live in a sad old SRO behind the University
23 Synagogue. There are some strange people in that
24 SRO. One of them is a guy who spent three years of
25 being on Rikers. Every time he has tried to attack

2 me, I call the 34. I'm sorry the 333—the 34 and I
3 ask for help and they come. The last time Officer
4 Bonhom came he swiped my ID in his new issued Table
5 that was paid for Cy Vance's Criminal Justice
6 Initiative dollars that were stolen from the people
7 of New York by the way. An alert comes up on their
8 tablet saying Ms. Price is no longer to receive
9 police services. I'm a fourth generation New Yorker.
10 My grandfather sailed on a ship from Columbia here in
11 1890. My grandfather served in the CIA. He served
12 in the OSS. I'm a 9/11 survivor. Why am I put on a
13 do not serve list? It's because somebody used my
14 data and fed it into the Palantir system as patient
15 zero as a fabricator. Do you know how amuck this
16 entire system has got? Who's serving information
17 into Palantir? Who is managing the Arrest Alert
18 System? Victims like me are marked to no longer
19 receive police services for forever. This psycho
20 that lives next door to me, he knows that. Something
21 needs to be done about this.

22 CHAIRPERSON GIBSON: Thank you very much.
23 Thank you.

24 YUNG MI-LEE: Thank you very much. My
25 name is Yung-Mi Lee and I'm supervising criminal

2 defense attorney at Brooklyn Defender Services. BDS
3 thanks the City Council Committee on Public Safety
4 and in particular Chair Vanessa Gibson for the
5 opportunity to testify in support of Intro 1482. We
6 also thank Council Member Dan Garodnick for
7 introducing the bill. In short, we strongly support
8 this bill. As a public defense organization, BDS is
9 principally concerned about the undisclosed use of
10 surveillance technologies and investigations against
11 our clients particularly those facing criminal
12 allegations and/or immigration enforcement. Give the
13 separate impact of law enforcement in general, it is
14 possible, if not likely, that these tools are
15 disproportionately used in low-income communities of
16 color. It is also possible that they have been used
17 without proper court authorization potentially
18 undermining the integrity of untold numbers of
19 criminal convictions. This common sense legislation
20 simply creates a measure of transparency so that
21 policy makers in the public can more fairly evaluate
22 it. It is important to understand that the vast
23 majority of police interventions in New York City are
24 not related to counter-terrorism, but summonses and
25 arrests for minor offenses in marginalized

2 communities under the Broken Windows Strategy.

3 Without transparency and accountability, it is

4 impossible for policy makers and the public to know

5 which police activities involve invasive and

6 sometimes costly surveillance tools and whether any

7 justifications offered by the NYPD are valid. Intro

8 1482 will help to provide this much needed

9 transparency. Policy makers and the public will then

10 have to ensure accountability. That said, one

11 crucial mechanism for both transparency and

12 accountability requires action in Albany. Repealing

13 the Blindfold Law and enacting meaningful-meaningful

14 criminal discovery reforms so that defendants and

15 their attorneys can see all the evidence and

16 information in their cases. Among the many

17 injustices, which—with our current criminal discovery

18 law, defense attorneys may be denied access not only

19 to the substance of the evidence collected in a

20 criminal case, but also the mechanism—the mechanisms

21 by which it is collected. Therefore, we rarely know

22 whether any of the surveillance technologies in

23 question are used against our clients, whether they

24 are used properly and in accordance with scientific

25 standards, and whether they are used with necessary

2 court authorization. Frankly, the courts might not
3 know that either. Repealing the state's Blindfold-
4 Blindfold Law, and passing meaningful discovery
5 reform will help to shine a light on these practices
6 in court. I also want to talk about ICE. BDS
7 greatly appreciated the provision in the bill
8 requiring reporting on the entities that have access
9 to the information and data collected by NYPD
10 surveillance technology, particularly as it relates
11 to federal immigration enforcement. ICE participated
12 in at least one joint operation with the NYPD last
13 year in which hundreds of officers raided a public
14 housing complex in the Bronx [bell] using military
15 grade weaponry. Other public housing raids have
16 involved both federal and local law enforcement
17 agencies as well. All of these raids were reportedly
18 based largely on surveillance of young men and boys
19 of color for several years beginning when some of
20 them were in middle school. Typically, several dozen
21 would be charged with racketeering and other
22 conspiracy charges stemming from comparatively few
23 alleged crimes and according to law enforcement,
24 seemingly capricious designations of alleged gang
25 involvement. Among other troubling aspects of these

2 raids, BDS is deeply concerned that NYPD surveillance
3 may be aiding in federal immigration enforcement not
4 only against alleged gangs members, but also anyone
5 else who may be caught up in the dragnet of these or
6 other investigations. Beyond-beyond these high
7 profile raids, we seek clarity on whether the NYPD's
8 broad network of surveillance technologies are openly
9 accessible to ICE and whether city resources are,
10 therefore, used to aid in federal government's mass
11 deportation effort. This common sense legislation
12 will shine a spotlight on practices that warrant
13 public scrutiny and debate. Thank you for your
14 consideration on comments. I respectfully urge the
15 Council to pass Intro 1482.

16 CHAIRPERSON GIBSON: Thank you very much.

17 TOWAKI KOMATSU: Hi. My name is and
18 Towaki Komatsu. I'm a U.S. Navy veteran. I'm going
19 to try to keep my comments pretty short and pretty
20 quick due to time constraints. First, the question I
21 have are what surveillance technology does the NYPD
22 have to confirm it flagrantly violated my civil
23 rights on April 27th, May 23rd and June 8th by
24 subjecting me to viewpoint discrimination in
25 violation of the Supreme Court 2014 decision in *Wood*

2 v. *Moss* and New York State's Open Meetings Law, and
3 unlawful force on April 27th, at the Mayor's Town
4 Hall in Long Island City by 108th Precinct Officer

5 Bito, Badge No. 13326. Question No. 2: What
6 surveillance technology does the NYPD have about
7 2000—the 2016 federal lawsuit filed against Howard
8 Redmond, who was the head of the Mayor's security
9 detail that I saw today outside the City Hall, for
10 civil rights abuse to substantiate the plaintiff's
11 claim in *Gerard v. City of New York* where that
12 lawsuit is still active at the Southern District.

13 Question 3: What surveillance technology does the
14 NYPD have that confirms Lieutenant Nieves of the
15 Intelligence Division violated Patrol Guide Procedure
16 No. 221-02 regarding excessive force by not asking if
17 I was injured after Officer Bito illegally shoved me
18 three times in the chest on a public sidewalk on 38th
19 Street in Long Island City on April 27th as he,
20 Officer Joel (sic) and a third officer watched and
21 stood next to Mr. Bito as he did that. The next
22 question is with regards to the comments about
23 Goldman Sachs today in this hearing, does Goldman
24 Sachs own New York City and NYPD or we the people?
25 Next question. What surveillance technology does the

2 NYPD have that confirms members of the NYPD illegally
3 asked court officers in the Bronx Supreme Court on
4 May 23rd, to keep this veteran out of Veterans
5 Memorial Hall at the Mayor's public meeting on that
6 date despite the fact that that NYPD has absolutely
7 no jurisdiction in a courthouse. Next question.
8 What surveillance technology does the NYPD have that
9 confirms Lieutenant Nieves stalked and eavesdropped—
10 eavesdropped on a private conversation I had with a
11 New York Post reporter. I think that was Michael
12 Gartman—Gartland in the hallway of that court on May
13 23rd while I was explaining to him that the NYPD was
14 illegally discriminating against me by keeping me out
15 of that—the Veterans Memorial Hall. I also have a
16 copy of the video footage from that date thanks to
17 OCA. If the NYPD operates under strict rules, as was
18 stated earlier, unfortunately not under the penalties
19 of perjury, why was the former tennis professional
20 thrown to the ground in front of Grand Hyatt, and why
21 can't Akai Gurley see his family now. Next question.
22 Who are New York City's real terrorists. [bell] And
23 I guess the last question is this: Why does this
24 veteran get to stand within 15 feet of the Mayor
25 outside of Borough Hall on April 11th where Officer

2 Joel let him do that, but when I tried to attend this
3 Town Hall event, and asked him as he was leaving the
4 Town Hall event on April 27th why Mr. Redmond had
5 illegally discriminated against me, if I was standing
6 45 feet away from him on April 27th, triple the
7 distance that I was standing away from where the
8 Mayor stood on April 11th. Why was I not allowed to
9 ask him a fundament question, why my fundamental due
10 process rights were violated on that date by keeping
11 me out of that public meeting in violation of New
12 York State's Open Meetings Law?

13 CHAIRPERSON GIBSON: Thank you very much.
14 Our next panelist. I know you just joined us. It's
15 Harlan Yu representing Upturn. Thank you for being
16 here. You may begin.

17 HARLAN YU: Good afternoon Chairperson
18 Gibson and members of the Committee on Public Safety.
19 My name is Harlan Yu and I'm a principal at Upturn.
20 We work with local and national civil rights groups
21 on issues where technology meets policing, and for
22 the last to years we've been focusing on body worn
23 cameras. Body worn cameras are powerful surveillance
24 tools. Whether or not cameras ultimately hold the
25 police more accountable, cameras will intensify

2 surveillance of New York's communities especially in
3 many communities of color where officers and cameras
4 will be most rampant. And instead of civil rights
5 principles and body worn cameras, a major collation
6 of civil rights and privacy groups in 2015 warned of
7 that, "There's a real risk that these new devices
8 could become instruments of injustice rather than
9 tools for accountability." We need not only strong
10 policy safeguards, but also transparency and public
11 oversight to ensure that cameras will serve the
12 interests of New Yorkers, and that's what the POST
13 Act would help to provide. The POST Act would help
14 to ensure on an ongoing basis that officers are
15 turning their cameras on and off when they're support
16 to and that footage is retained, secured and accessed
17 according to the department's policy. Strong public
18 oversight is all the more important for fast changing
19 technologies like body worn cameras. Right now, The
20 View, the vendor, which supplies cameras to the NYPD
21 is building face recognition technologies, and other
22 automated search capabilities into their system.
23 This would give the NYPD the power to automatically
24 scan and search every face that a body camera sees,
25 and would quickly turn body cameras into a system of

2 intense localized mass surveillance. Even though the
3 city's body camera program is subject to some
4 judicial oversight through *Floyd*, that is no
5 substitute for what the POST Act would require, and
6 in particular Judge Torres only has jurisdiction over
7 the NYPD's One-Year Pilot Program, and after the
8 first year, the NYPD could incorporate face
9 recognition into the body cameras without telling the
10 judge, without telling the members of this committee
11 and without telling the public. These powerful new
12 capabilities should not be adopted in secret. The
13 POST Act would provide the public with meaningful
14 safeguards without compromising public safety. It
15 would simply require the NYPD to explain how it
16 intends to use the technology, and give New Yorkers a
17 chance to weigh in. The POST Act is a balanced and
18 common sense proposal that would shed important light
19 on the NYPD's most invasive practices. Thank you.

20 CHAIRPERSON GIBSON: Thank you very much.
21 Thank you all for coming today, and for sharing your
22 story.

23 FEMALE SPEAKER: Could I ask you a
24 question? Could I testify as a private citizen
25 because I was testifying as a group I belong to, but

2 hearing what the NYPD said, I would like to offer a
3 testimony as a computer hacker and a private citizen
4 of New York City since 1992.

5 CHAIRPERSON GIBSON: Okay.

6 FEMALE SPEAKER: Could you allow me my
7 three minute on that?

8 CHAIRPERSON GIBSON: Well, I'm sorry.
9 Well, we have to close the hearing because there's
10 another hearing coming behind us.

11 FEMALE SPEAKER: It's very quick.

12 CHAIRPERSON GIBSON: So if there's
13 anything you want to submit, you're able to do that
14 at another time after the hearing closes. You can
15 submit written testimony.

16 FEMALE SPEAKER: Oh, because it seems
17 there was no testimony from housing experts or a
18 computer hacker like myself. So, I just wanted to--

19 CHAIRPERSON GIBSON: Okay, yeah, you can
20 submit it as-in written format. Okay?

21 FEMALE SPEAKER: Okay.

22 CHAIRPERSON GIBSON: Thank you so very
23 much. Thank you. Thank you everyone for coming. I
24 want to also acknowledge for the record that we've
25 received testimony from the Neighborhood Defender

2 Service, NDS of Harlem in support of Intro 1482, and
3 once again I wan to thank the members of the City
4 Council, our prime sponsor Council Member Dan
5 Garodnick, and want to thank him and his staff.
6 Thank you to all my colleagues who were here. Thank
7 you to the NYPD for their presence and testimony as
8 well as all the advocacy groups and stakeholders, and
9 legal service providers. Thank you to the sergeant-
10 at-arms, and thank you to our staff. We look forward
11 to having further conversations on Intro 1482 and its
12 passage in the City Council. Thank you all for being
13 here. Thank you to the sergeant-at-arms and this
14 hearing of the Committee on Public Safety is hereby
15 adjourned. Thank you. [gavel]

16

17

18

19

20

21

22

23

24

25

C E R T I F I C A T E

World Wide Dictation certifies that the foregoing transcript is a true and accurate record of the proceedings. We further certify that there is no relation to any of the parties to this action by blood or marriage, and that there is interest in the outcome of this matter.



Date July 9, 2017