

CITY COUNCIL
CITY OF NEW YORK

----- X

TRANSCRIPT OF THE MINUTES

Of the

COMMITTEE ON PUBLIC SAFETY

Jointly with

COMMITTEE ON TECHNOLOGY

----- X

December 15, 2023
Start: 1:11 p.m.
Recess: 4:39 p.m.

HELD AT: Council Chambers - City Hall

B E F O R E: Kamillah Hanks
Chairperson

Jennifer Gutiérrez
Chairperson

COUNCIL MEMBERS: Joann Ariola
Erik D. Bottcher
Justin L. Brannan
Tiffany Cabán
Carmen N. De La Rosa
Robert F. Holden
Rita C. Joseph
Darlene Mealy
Althea V. Stevens
Shaun Abreu
Ari Kagan
Vickie Paladino
Julie Won

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

Jeffrey Maddrey
NYPD Chief

Michael Gerber
NYPD Deputy Commissioner

Michael Fitzpatrick
Chief Privacy Officer at Office of Technology and
Innovation

Seth Severino
NYPD Assistant Deputy Commissioner

Emily Gold
NYPD Chief Privacy Officer

Melanie Braverman
NYPD Managing Attorney

Nicholas Mendoza
NYPD Chief Contracting Officer

Jocelyn Strauber
DOI Commissioner

Michael Sisitzky
New York Civil Liberties Union

Jerome Greco
New York Legal Aid

Nina Loshkajian
STOP

Johnathan Lamb
Amnesty International

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

Ivey Dyson
Brennan Center for Justice

Elizabeth Vasquez
Brooklyn Defender Services

1 <INSERT TITLE OF MEETING>

4

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

2 SERGEANT AT ARMS: Good afternoon and
3 welcome to the Committees on Public Safety jointly
4 with Technology. At this time, we ask that you
5 please place phones on vibrate or silent mode. Thank
6 you, Chairs. We are ready to begin.

7 CHAIRPERSON GUTIÉRREZ: Good afternoon
8 and welcome to our hearing. I'm Council Member
9 Jennifer Gutiérrez, and I'm the Chair for the
10 Committee on Technology. I'm pleased to join Council
11 Member Hanks for this hearing on the critically
12 important POST Act. I appreciate the opportunity to
13 discuss a matter of paramount importance, the New
14 York Police Department's compliance with the public
15 oversight of surveillance technology, also known as
16 the POST Act. I come to this hearing with both
17 gratitude and concern. Gratitude because the POST
18 Act represents a pivotal step forward in our
19 society's commitment to transparency and
20 accountability, and the use of surveillance
21 technologies by our law enforcement agencies.
22 Concerns, because we haven't been able to meet the
23 goals laid out in the legislation, and compliance has
24 not been fully achieved. The POST Act was crafted
25 with the intent of creating a balance between public

2 safety and the fundamental safeguarding of civil
3 liberties. It requires the NYPD to provide clear and
4 comprehensive guidelines regarding the deployment and
5 implications of surveillance technology. With
6 technology's constant and rapid development, it's
7 vital that our regulations keep pace through the good
8 governance measures of transparency and
9 accountability. However, NYPD's own office of the
10 Inspector General, OIG, found that PD was not in full
11 compliance with the POST Act. Instead, OIG determined
12 that NYPD had taken advantage of loopholes and
13 ambiguities to evade essential transparency measures.
14 As the City Council we are responsible for ensuring
15 that the NYPD fully adheres to the principles and
16 requirements of the POST Act. Instead, OIG
17 determined that NYPD-- oh, wait. We are
18 responsible-- sorry, the POST Act. To this end, we
19 are convening to also discuss several bills that will
20 fortify the law and ensure its robust enforcement.
21 In addition to understanding what technologies the PD
22 is using, we also need transparency into how the PD
23 uses data sharing agreements, how long it retains
24 data, and whether information is shared with other
25 agencies or entities including federal law

1 enforcement. Transparency in these matters is not
2 merely a technical matter of compliance, but a
3 hallmark of responsible governance. It is imperative
4 that we examine the use of certain technologies such
5 as aerial drones and the subway Robocop, and
6 understand why the NYPD has not issued impact and use
7 policies for these clearly novel technologies. This
8 merits further scrutiny and may warrant future
9 amendments to existing legislation. We must also
10 consider the role of the Office of Technology and
11 Innovation in oversight and risk management. OTI has
12 testified that they are responsible for agency's
13 technology procurement and management, a critical
14 issue that we are exploring here today. How does OTI
15 inform the NYPD solicitation for new technology? How
16 does OTI ensure that surveillance technology are
17 audited and scrutinized effectively, and what
18 mechanisms are in place to guarantee that these tools
19 are used responsibly and within the boundaries of the
20 law? We hold these hearing not as adversaries, but
21 as stewards for the public trust. The concerns about
22 the lack of transparency come both from multiple
23 branches of city government and outside of it. Our
24 objective is clear, to ensure that the POST Act
25

2 fulfills its intended purpose of providing
3 transparency and accountability in the use of
4 surveillance technology by the NYPD. It is our
5 collective duty to protect the rights and privacy of
6 our citizens while also upholding the principles of
7 public safety. Given the accommodations these
8 committees provided to the NYPD in the rescheduling
9 of this hearing, we're looking forward to NYPD's full
10 engagement with questions from Council Members, as
11 well as listening to testimony from the public. I
12 hope you will stay as long as you can, and I look
13 forward to the insights that will emerge from this
14 hearing as we work together to achieve these crucial
15 objectives, and I like to recognize Technology
16 Committee Members who are present, Council Member
17 Abreu-- and that's it. I'll pass it over to Chair
18 Hanks.

19 CHAIRPERSON HANKS: Thank you so much,
20 Chair Gutiérrez. Good afternoon. Happy Friday and
21 happy holidays. I am Council Member Kamillah Hanks.
22 I'm the Chair on the Committee of Public Safety, and
23 again, I am joined by Chair Gutiérrez of the
24 Technology Committee and Public Safety Members and
25 Council Members Abreu, Cabán, Bottcher, and we are

2 also joined by our Public Advocate. Welcome to
3 today's joint hearing of the Public Safety and
4 Technology Committee where we'll be examining the
5 NYPD's use of surveillance and implementation of the
6 Public Oversight Surveillance Technology Act, the
7 POST Act. We will also be hearing related
8 legislative proposals aimed at enhancing transparency
9 and the NYPD's use of surveillance and improving
10 privacy safeguards and oversight in the Department's
11 use of surveillance. The New York City Police
12 Department relies on a wide array of surveillance
13 technologies to fulfill its mission in maintaining
14 public safety. These technologies have the potential
15 to gather vast amounts of personal data and their--
16 and they raise valid concerns about potential impacts
17 on privacy and civil liberties of civilians. To
18 address some of those concerns, this council enacted
19 the POST Act in 2020 which designed-- which was
20 designed to provide oversight regarding NYPD's
21 acquisition of use of surveillance technologies.
22 Specifically, the POST Act mandates that NYPD publish
23 impact and use policies, IUPs, for all surveillance
24 technologies used by the Department and continually
25 produce IUPs upon the acquisition of new

2 technologies. As required by the POST Act, the IUPs
3 must provide detailed information about the
4 technology's capacities, capabilities, Department
5 guidelines on access and such use of technologies,
6 data sharing and retention policies and more. The
7 POST Act also requires the opportunity for the public
8 to have input on all draft IUPs to provide a one--
9 excuse me-- a 45-day period for public comment on
10 draft policies in order to have public concerns taken
11 into account when NYPD creates its final policy. The
12 NYPD has made great strides in publishing the IUPs
13 for various surveillance technologies covering a wide
14 range of capabilities. However, the recent
15 evaluations by the Office of Inspector General for
16 NYPD raised shortcomings in published policies.
17 Notably, the OIG/NYPD described generic boiler plate
18 language used in the majority of the IUPs and the
19 grouping of related technologies under the single
20 IUPs which impeded the inspector General's ability to
21 conduct meaningful oversight and audits of the
22 Department's use of surveillance as required by the
23 POST Act. Our goal for this hearing is to assess the
24 NYPD's progress in implementing the POST Act,
25 consider legislative enhancements to the Act, to hear

2 public-- to hear concerns of the public and examine
3 how NYPD seeks to maintain a delicate balance between
4 using surveillance to secure public safety while
5 ensuring civil liberties. Additionally, at this
6 hearing we will be hearing-- we will-- considering
7 and hearing four pieces of legislation in the Public
8 Safety Committee, Intro 1193 sponsored by Council
9 Member Fariás, legislation to strengthen the
10 OIG/NYPD's capacity to conduct meaningful audits of
11 eh NYPD published IUPs. Intro 1195, sponsored by
12 Council Member Hudson, legislation to require NYPD to
13 publish a written policy that establishes procedures
14 and regulations for its use of facial recognition
15 technologies and conduct biannual public audits of
16 the Department's use of facial recognition
17 technology. And Intro 1207 sponsored by Council
18 Member Won, legislation to amend the existing POST
19 Act to ensure IUPs contain sufficient detail and
20 specificity needed to enable meaningful oversight and
21 regular audits. Finally, we will hear Intro Number
22 1047, sponsored by Council Member Vernikov, in
23 relation to requiring-- okay, we will not be doing
24 that. I was just patted. So, to that end, I would
25 like to again thank Council Member Gutiérrez, Chair

2 of the Committee on Technology, our staff for all the
3 hard work for putting this hearing together, and I
4 look forward to an engaging and constructive dialogue
5 with all stakeholders including representatives from
6 the Administration, advocates and members of the
7 public to chart a pathway forward that best serves
8 all of New Yorkers. Thank you for your participation
9 in this critical discussion. And now I'll turn it
10 over to our public advocate for his opening
11 statement. Thank you so much.

12 PUBLIC ADVOCATE WILLIAMS: thank you,
13 Madam Chair. As mentioned, my name is Jumaane
14 Williams. I'm the Public Advocate for the City of
15 New York. I want to thank Chair Gutiérrez and Chair
16 Hanks and the Committee members for holding this
17 hearing. Fundamentally, everyone is protected by the
18 14th amendment's right to privacy in the United
19 States Constitution. While New York Police
20 Department has the responsibility to secure the
21 safety of New Yorkers, we also must be extremely
22 cautious in adapting technology that violates civil
23 rights. We all know that technology is coming. It
24 is not something that we could prevent. We have to
25 make sure that it is instituted while honoring civil

2 rights. Individuals should have reasonable
3 expectations that they can move around freely without
4 overuse of surveillance by law enforcement. Law
5 enforcement agencies that recently adopted facial
6 recognition technology are also being sued for racial
7 and gender discrimination. Detroit has seen three
8 lawsuits for wrongful arrest stemming from facial
9 recognition technology. Researchers at MIT reported
10 in January 2019 that facial recognition software
11 marketed by Amazon, mis-identified darker-skinned
12 women 31 percent of the time. While other studies
13 have shown, "shown that algorithms used in facial
14 recognition return false at a higher rate for
15 African-Americans and white Americans unless
16 explicitly recalibrated for a black population."
17 Specifically the Amazon technology mis-identifies
18 people with dark complexion 15 percent of the time,
19 as compared to only three percent for people with
20 light complexions. These findings prompted experts
21 at Google, Facebook, and Microsoft to sign a letter
22 calling on Amazon to stop selling its facial
23 recognition technology to law enforcement. With mass
24 surveillance, personal information is more likely to
25 be at risk. It is no exaggeration to say that leaks

2 of personal data can put people's lives at risk,
3 commuting patterns, frequent locations or other
4 identifying information threatens survivors of
5 domestic violence as well as anyone in a marginalized
6 group who may be targeted. For example, an Anchorage
7 police officer used an internal database to find and
8 sexually assault a woman. How the NYPD uses
9 technology must be closely monitored and abusers held
10 accountable. Additionally, hacking may not even be
11 necessary for those looking to cause harm.

12 Surveillance contractors often sell their data to
13 third parties which leads to poorly monitored
14 databases being created. I want to thank my
15 colleagues for introducing legislation that will
16 create more accountability and transparency around
17 the police's use of technology. Strict monitoring is
18 necessary to oversee the NYPD's vast tool kit of
19 surveillance technologies. There's reason to be
20 concerned when NYPD utilizes many technologies such
21 as robot police officers in Times Square, drones at
22 crime scenes, x-ray vans, and GPS tracking allowing
23 officer [sic] to tag and track vehicles without
24 oversight of how these technologies are stored and
25 tracking data on New Yorkers. The NYPD opting into

2 the Amazon Ring program itself is cause for concern.

3 Ultimately, the council must take concrete steps to

4 limit the use of facial recognition technology in the

5 future when it comes to better policing, just like

6 better education, better medication, better medicine.

7 This is a conversation that always has to continue.

8 I don't think it would ever stop, nor should it, and

9 I hope these conversations could happen with that

10 spirit in mind. Lastly, we mentioned the tragic

11 event that happened yesterday where technology was

12 used. Unfortunately, we still saw a fatality, and a

13 police officer shot. Thankfully, that officer was

14 wearing his bullet-proof vest and will go home to his

15 family. [inaudible] was barricaded and was killed.

16 But technology was used there. Unfortunately, we

17 still had a familiar outcome. Thank you.

18 CHAIRPERSON GUTIÉRREZ: Thank you so

19 much. Okay, you can swear in folks.

20 COMMITTEE COUNSEL: Welcome everyone.

21 From the Administration we'll be hearing testimony

22 from the NYPD and the Office of Technology and

23 Innovation to begin with. From NYPD we have Chief

24 Jeffrey Maddrey and Deputy Commissioner Michael

25 Gerber, and for Office of Technology and Innovation

2 we have Michael Fitzpatrick. There's a bunch of
3 other folks who are going to be available for
4 question and answer for NYPD, which is Assistant
5 Deputy Commissioner Seth Severino, Chief Privacy
6 Officer Emily Gold, Managing Attorney Melanie
7 Braverman, and Chief Contracting Officer Nicholas
8 Mendoza. So, can you all just raise your right hand
9 and affirm the following? Do you affirm to tell the
10 truth, the whole truth and nothing but the truth and
11 to answer honestly to Council Member questions?
12 Acknowledge that you all have said yes. So, you may
13 begin.

14 DEPUTY COMMISSIONER GERBER: Good

15 afternoon chair Hanks, Chair Gutiérrez and members of
16 the Council. My name is Michael Gerber, and I'm the
17 Deputy Commissioner of Legal Matters for the NYPD.
18 Since the POST Act was passed in 2020, the NYPD has
19 worked to meet its obligations under the law. Within
20 180 days after the passage of the Act, the Department
21 published 36 draft impact and use policies, or IUPs,
22 containing more than 300 pages of information
23 regarding the Department's surveillance technologies.
24 Following a comment period, the IUPs were finalized
25 in April 2021. The IUPs are publicly available on our

2 website and provide a wide range of information
3 concerning capabilities of our surveillance
4 technologies, as well as policies and procedures
5 relating to those surveillance technologies. Through
6 release of our IUPs and subsequent amendments have
7 dramatically increased the Department's public
8 disclosures regarding its surveillance technologies.
9 The POST Act strikes a balance between a number of
10 critical interests, transparency, public safety,
11 innovation, and administrability [sic]. We disclose
12 a wide range of information without compromising our
13 ability to solve crimes and keep people safe. It has
14 been suggested that we are grouping multiple
15 surveillance technologies within a single IUP in a
16 manner that undermines transparency. That is not the
17 case. Within a given surveillance technology there
18 will be different types of equipment and models,
19 various forms in which the surveillance technology
20 may be deployed, and a range of uses for that
21 surveillance technology. We have not done a separate
22 IUP and comment period for each type of hardware that
23 deploys a given surveillance technology. Such an
24 approach is not required by the POST Act. Having a
25 separate IUP for each brand of camera that we use or

2 each variation on a given type of surveillance
3 technology would result in repetition and confusion.
4 In fact, it would decrease transparency. The nature
5 of a particular surveillance technology used by the
6 Department would be scattered across multiple IUPs.
7 It would also be administratively unworkable.
8 Itemizing surveillance technology using covert
9 operations would endanger public safety, provide a
10 detailed road map to those who wish to do harm, and
11 put our undercovers at risk. The POST Act accounts
12 for all this. It makes clear that each surveillance
13 technology must be covered within an IUP, but that
14 enhancements to a surveillance technology, or the
15 deployment of a surveillance technology for a new
16 purpose, or in a new manner do not result in a new
17 IUP and comment period. Rather, the Department is to
18 write an addendum to a pre-existing IUP. I want to
19 emphasize that in these circumstances, proceeding by
20 addendum rather than doing a new IUP is not contrary
21 to the POST Act. It is what the POST Act mandates,
22 and it gives the Department the flexibility to use
23 pre-existing surveillance technology in new ways,
24 while maintaining transparency with the public. I
25 would now like to take a moment to comment on the

2 bills being heard today. Intro 1193 would require
3 the Department to provide to DOI upon a request a
4 list of surveillance technologies, information on
5 data access and retention policies, and quarterly
6 updates on new and discontinued technologies. The
7 Department takes DOI's oversight mission very
8 seriously and works with DOI to ensure that they can
9 fulfill that mission. We are committed to continuing
10 to do so. The Department looks forward to working
11 with the Council to craft this legislation, and to
12 ensure that DOI has the information it needs to
13 fulfill its audit function. Intro 1195 would require
14 the Department to establish and publish procedures
15 and regulations for the use of facial recognition
16 technology. The bill would also require the
17 Department to conduct biannual audits of our use of
18 facial recognition, and to provide the results to
19 DOI, as well as publish them on our website. I would
20 note that the section of the patrol guide addressing
21 facial recognition is posted on the Department's
22 website, together with answers to frequently asked
23 questions regarding our use of facial recognition is
24 posted on the Department's website together with
25 answers to frequently asked questions regarding our

2 use of facial recognition. We have no issue with
3 continuing to publicize this information and we are
4 open to providing more data regarding our use of the
5 surveillance technology. We would, however, like to
6 have a dialogue with the Council regarding the
7 contours and scope of the audit. The bill as
8 presently drafted requires granular detail regarding
9 each itemized use of facial recognition technology,
10 and that at least at present, is administratively
11 unfeasible and could interfere with our ability to
12 use this important law enforcement tool. We believe
13 that we can work with the Council to craft an audit
14 that will further increase transparency without
15 impeding critical law enforcement efforts. Intro
16 1207 would require a separate IUP for each
17 surveillance technology used by the NYPD regardless
18 of whether such technology overlaps in functionality
19 or capability with any other technology for which an
20 IUP already exists. We aren't sure what is intended
21 by this language. Does this mean that every time the
22 Department intends to purchase a different make or
23 model of camera with even slightly altered
24 functionality, a new IUP would have to be issued? We
25 replace officer's smartphones, would a new IUP be

2 required? Does this mean that the Department would be
3 required to do an IUP for a new covert undercover
4 recording device? These are not rhetorical
5 questions. The language of the bill as presently
6 drafted is unclear. If the answer to these questions
7 is yes, the bill would be extremely harmful to the
8 functioning of the Department and could serve to
9 compromise public safety. The Department opposes
10 this legislation as drafted, because it would upset
11 the careful balance that lies at the heart of the
12 POST Act. We look forward to a continuing dialogue
13 with the Council regarding the proposed bills, and
14 more generally, regarding the POST Act. Thank you
15 for the opportunity to testify on this matter, and we
16 look forward to answering any questions you may have.

17 CHAIRPERSON HANKS: Thank you so much,
18 and thank you all for all the hard work that you do
19 for this city. We just want to recognize that
20 publicly. Before I get into questions, I would love
21 to recognize Council Member Joseph, Ariola, Paladino,
22 Holden, and Mealy have joined us. So can you provide
23 an overview of the surveillance technologies
24 currently used by the NYPD?

2 CHIEF MADDREY: [inaudible] Good

3 afternoon. I think when you look at our surveillance
4 technology, some of our more widespread technology
5 that we use is of course our license plate readers,
6 our Argus [sic] cameras, our body-worn cameras
7 assigned to our officers, I think those are our most
8 widespread used technology that we have in the
9 Department that's used on a daily basis. And then
10 when you drill down, we have been implementing
11 drones. Of course, we use cameras fixed and mobile.
12 And you know, you touched on facial identification,
13 but I think that's pretty much the big picture. I
14 mean, we could drill down more, but that's the big
15 picture of what we use on a daily basis.

16 CHAIRPERSON HANKS: Thank you.

17 Commissioner, you testified that if we would have a
18 report for each IUP, that it would decrease
19 transparency as the nature of the particular
20 surveillance that is used by the Department would be
21 scattered across multiple. And you know, for
22 administratively, itemizing surveillance technologies
23 used in covert operations would endanger public
24 safety. Talk a little bit about this specifically
25 for the public to understand what that actually mean.

2 It's in the second paragraph of your testimony. I
3 think we should just like kind of unpack that a
4 little bit.

5 DEPUTY COMMISSIONER GERBER: Sure,
6 absolutely.

7 CHAIRPERSON HANKS: Thanks.

8 DEPUTY COMMISSIONER GERBER: So, for each
9 surveillance technology we have an IUP. Now, for any-
10 - for a given surveillance technology, that could be
11 deployed in different ways. So for example,
12 situational awareness cameras, we can deploy these
13 cameras in a variety of context. You could have
14 different platforms, different purposes for which we
15 use those cameras. If we were to have a separate IUP
16 for each type of camera that we use, or each
17 different place where we could put a camera, or each
18 different way we could deploy a camera, that's not
19 what the POST Act requires, but it also would be
20 incredibly difficult for the public to understand
21 what's being done. Other words, as it stands now, if
22 a member of the public wants to understand how we're
23 using situational awareness cameras, they can go look
24 at the situational awareness camera IUP and that will
25 lay that out. If we had numerous IUPs for each

2 different type of camera-- again, putting aside the
3 administrability [sic] issue-- you'd have tremendous
4 repetition, obviously across the IUP. You'd have
5 tremendous overlap, but also I don't think a member
6 of the public would know where to look. Is it this
7 type of camera? Is it that type of camera? They're
8 actually now-- you're a member of the public and you
9 want to understand a variety of matters regarding a
10 given surveillance technology. You go to the IUP for
11 that surveillance technology, and then you can learn
12 more about it in a variety of ways.

13 CHAIRPERSON HANKS: Thank you. So, also
14 to a little dig deeper into that, you also testified
15 that the Department is now required to write an
16 addendum to a pre-existing IUP. What is the
17 timeframe for submitting such addendums, and how many
18 addendums if any have been done thus far? Would you
19 happen to have that information?

20 DEPUTY COMMISSIONER GERBER: Yes. So,
21 the statute actually does not give a timeframe for
22 the addendum. The statute is silent on that. And
23 you know, we have undertaken to do that, frankly and
24 we try to do it in a reasonable timeframe, in a fair
25 timeframe, but the statute actually is silent on that

2 matter. With regard to which IUPs we've done
3 addendums to, I can tell you, it's body-worn cameras,
4 cell side [sic] simulators, CCTV systems, Calia [sp?]
5 Collection system, the criminal group database,
6 digital fingerprint scanning devices, facial
7 recognition, portable electronic devices, situational
8 awareness cameras, thermographic cameras, and
9 unmanned aircraft systems. So we have done
10 addendums, additional information has been provided
11 with regard to each of those IUPs over time.

12 CHAIRPERSON HANKS: Thank you so much.

13 Does the NYPD track to the extent of which the data
14 is gathered by surveillance technologies and they're
15 shared with external entities?

16 DEPUTY COMMISSIONER GERBER: I'm not sure
17 I understand the question exactly.

18 CHAIRPERSON HANKS: So, does the NYPD
19 have specific data sharing and retention policies? I
20 apologize, I kind of jumped the question before
21 really kind of unpacking it for you. I apologize.
22 So, you know, do we have specific data sharing and
23 retention policies for the use of data gathered
24 through surveillance technologies? Are there
25 uniformed policies and protections in the terms and

2 agreements with external entities? And then I moved
3 into saying do we have a policy on how we share.

4 DEPUTY COMMISSIONER GERBER: Right, so
5 there are a number of different pieces to that. So,
6 first of all, we obviously do have a set of rules,
7 whether by statute or by, you know, a policy
8 regarding data retention, personal identifying
9 information. There's a whole set of rules about
10 that. And I should say, by the way, that those sets
11 of rules are going to be at least as a baseline
12 matter consistent across multiple IUPs. Which is one
13 of the issues with regard to, you know, boiler plate,
14 I think it's important to emphasize-- this was
15 mentioned earlier-- it's not boiler plate. It's our
16 policies. And it is a great example. We're going to
17 have a baseline set of rules and regulations about
18 data privacy, data security that are going to be
19 consistent across our IUPs and across the
20 Departments. That's a good thing. So, I do want to
21 say that-- we can come back to this maybe, but on the
22 boiler plate pieces, it's not boiler plate, it's the
23 consistency that I think one would want across an
24 organizations to have baselined rules and regulations
25 that apply, and then for particular IUPs, maybe

2 additional-- but for particular surveillance
3 technologies, there might be additional rules,
4 restrictions on top of that. But coming back to your
5 question-- so there are rules about our ability to
6 share information, obviously. We do share
7 information with law enforcement partners in the
8 course of criminal investigations. That does happen,
9 of course. I should emphasize that we think of that
10 in terms of investigations. We organize that by
11 investigations, not by surveillance technology. If
12 we are partnering with a federal, state, or local law
13 enforcement agency on a particular investigation,
14 obviously they're sharing between the law enforcement
15 partners as one would expect. With regard to, you
16 know, vendors or third parties where we have, you
17 know, contracts, that is a standard, I think it's
18 exhibit A that is appended to these contracts that
19 has our standard rules regarding data privacy and
20 data sharing. I think that's actually available
21 online. And that's like a standard form that we use
22 in a wide variety of agreements with third parties.

23 CHAIRPERSON HANKS: Thank you so much.

24 So, when you're gathering this data, does NYPD ever
25 use this for commercial purposes?

2 DEPUTY COMMISSIONER GERBER: the NYPD?

3 No, absolutely not.

4 CHAIRPERSON HANKS: Okay, great thanks.

5 So how does NYPD seek to balance the demands for
6 public transparency regarding its use of surveillance
7 technologies where the Department needs to protect
8 sensitive information regarding operational
9 protocols?

10 DEPUTY COMMISSIONER GERBER: Right, we're
11 very sensitive to that. Obviously, transparency is
12 crucial. There are, of course, obviously, public
13 safety issues and there's a balance there. And you
14 know with regard to our POST Act IUPs, we do try to
15 provide a lot of information about our technologies.
16 Obviously, always can provide more detail and if
17 there's a question of line drawing that always exists
18 when you're doing this, and we do try to strike that
19 balance. We want to provide the information called
20 for. We need to provide the information called for
21 by the POST Act, and we do that, but when we-- we
22 drafted the IUPs, and when we do the addendums to the
23 RFPs, we are sensitive not to compromise on public
24 safety when we're doing that.

2 CHAIRPERSON HANKS: Thank you. The NYPD,
3 you also previously expressed concerns about the
4 extent to which disclosure of these surveillance
5 technologies can impede the ability to conduct
6 investigations. Can you provide specific examples of
7 how disclosing information requires by the POST Act
8 could reveal vulnerabilities and compromise
9 intelligence operations?

10 DEPUTY COMMISSIONER GERBER: I want to be
11 very clear, I think that the way the POST Act is
12 written now, I don't think it calls for that. I have
13 concerns that the POST Act could be amended in a way
14 that would raise those issues. So, just to take an
15 example, we have an IUP for covert recording devices
16 and exchange information about rules, policies, how
17 we might use covert recording devices. We do not
18 list out in the IUP or otherwise publicly the
19 different types of locations or places where an
20 undercover might have a covert recording device for
21 obviously reasons. Now, that is consistent with the
22 POST Act as written, and I-- we're very comfortable
23 with that. I do have concerns that Intro 1207,
24 again, I think the language it's not clear what's
25 intended, and I-- we're genuinely unsure about that.

2 But when you start talking about doing a new IUP for
3 anything, any surveillance technology utilized by the
4 Department, even if there's an overlap in
5 functionality or capability, I think it raise a
6 question at least. Is that demanding that each time
7 we find a new place to put a covert recording device,
8 on an undercover, we have to do an IUP for that? I
9 find it difficult to imagine that that's what's
10 intended. I think the language could be read that
11 way, though.

12 CHAIRPERSON HANKS: Yeah, I could read it
13 that way. I'm going to ask a few other questions,
14 and then we're going to take a two-minute break to
15 kind of switch gears. And this is really surrounding
16 around public notice, you know, and comments. What
17 are the protocols in place to provide the public with
18 notice about newly acquired and deployed surveillance
19 technologies?

20 DEPUTY COMMISSIONER GERBER: So, if you
21 renew surveillance technology, the POST Act
22 essentially requires 90-day-- you do a draft IUP, and
23 then there's a 45-day comment period. The draft IUP
24 is published, available to the public, and then
25 individuals can comment on it, and then it's at least

2 another 45 days until the IUP becomes final. So when
3 you have a new surveillance technology, there's this
4 sort of comment period the POST Act provides for.
5 When you have not a new surveillance technology, but
6 a pre-existing surveillance technology that's being
7 deployed in a new manner or for a new purpose, or
8 even when there's an enhancement to that surveillance
9 technology, what the POST Act says is you don't have
10 to do a new IUP, you don't have to have a comment
11 period. You do an addendum to the publicly available
12 IUP, and that way the public is told, hey, we are
13 taking this pre-existing surveillance technology, and
14 we are deploying it in a new manner or for a new
15 purpose, or with some enhancement.

16 CHAIRPERSON HANKS: Thank you so much.
17 I'm going to conclude my first round and I'm going to
18 pass it along to Chair Gutiérrez next.

19 CHAIRPERSON GUTIÉRREZ: Thank you so
20 much, Chair. And I know we have limited time and I
21 know members have questions, so I will do a couple of
22 questions and then pass it on to members so they can
23 get their questions in. So, I wanted to ask if you
24 could expand a little bit on the data sharing
25 question that Chair Hanks asked. Would you be able

2 to tell me with more details kind of how the--
3 whatever data is collected from any and all of the
4 surveillance devices, how you all determine, you
5 know, which agencies or external or third party
6 agencies get which data?

7 DEPUTY COMMISSIONER GERBER: Sure. So
8 there is a whole set of rules about that. We have
9 our agency Privacy Officer here, and-- Emily Gold,
10 and if it's okay, she can come to the microphone and
11 answer your question.

12 CHAIRPERSON GUTIÉRREZ: Yeah, I would
13 love that. And I'd also like to recognize Council
14 Member De La Rosa, Althea Stevens, and Council Member
15 Darlene Mealy, and Council Member Erik Bottcher, and
16 Bob Holden [inaudible].

17 CHIEF PRIVACY OFFICER GOLD: Hi, good
18 afternoon. So, in terms of how we determine whether
19 data is shared, that's really a request that comes
20 from an operational standpoint, and then its assessed
21 by relevant operational commands and for legal
22 concerns which is where I come in to determine
23 whether or not we're allowed to share the information
24 under-- as the agency Privacy Officer and looking at
25 the identifying information law and whether or not

2 identifying information is being asked for, and
3 whether we can be giving it under the citywide
4 guidance.

5 CHAIRPERSON GUTIÉRREZ: So, have there
6 been instances where you have been sharing where--
7 the agency has been sharing data?

8 CHIEF PRIVACY OFFICER GOLD: Yeah, we
9 share data.

10 CHAIRPERSON GUTIÉRREZ: Okay, and what
11 are-- can you share what-- which agencies?

12 CHIEF PRIVACY OFFICER GOLD: Well, we--
13 across the board we share data broadly. If you're
14 looking-- if we're focusing down on POST Act
15 technologies and kind of surveillance technologies, I
16 think the most relevant data shares would be with our
17 case management systems, because that's how-- sorry?

18 CHAIRPERSON GUTIÉRREZ: Still internally
19 with PD?

20 CHIEF PRIVACY OFFICER GOLD: Well, you're
21 asking for sharing outside of the agency?

22 CHAIRPERSON GUTIÉRREZ: Yes. Well, I'm
23 asking-- yes, exactly.

24 CHIEF PRIVACY OFFICER GOLD: Right.

2 CHAIRPERSON GUTIÉRREZ: All other
3 agencies.

4 CHIEF PRIVACY OFFICER: Right, so we
5 share information on our case management systems with
6 like the prosecutor's offices, because that's how
7 they get the information they're-- that we have to
8 give them for discovery demands. Similarly, that's
9 how-- that is how and why we share like body-worn
10 camera footage as well.

11 CHAIRPERSON GUTIÉRREZ: Okay.

12 CHIEF PRIVACY OFFICER GOLD: all of that
13 is governed by-- and every day the share is governed
14 by an agreement that outlines how the data is
15 transferred, like technologically, and how it is
16 meant to be utilized, stored, and limits its use by
17 the other entity and what they're allowed to do with
18 it.

19 CHAIRPERSON GUTIÉRREZ: Are there
20 instances where data is shared with-- outside of city
21 agencies, federal agencies or third parties?

22 CHIEF PRIVACY OFFICER GOLD: Federal
23 agencies, most of our sharing is actually for ongoing
24 investigations. It's a lot of-- with our taskforces.
25 So, like our federal taskforces like FBI. That is

2 also done by MOU, but most of that information is
3 being shared during an ongoing and open
4 investigation.

5 CHAIRPERSON GUTIÉRREZ: Okay. And what
6 about ICE?

7 DEPUTY COMMISSIONER GERBER: Absolutely
8 not.

9 CHIEF PRIVACY OFFICER: No, right? Yeah,
10 we don't share.

11 DEPUTY COMMISSIONER GERBER: We do not
12 share any of the surveillance technology data with
13 ICE.

14 CHAIRPERSON GUTIÉRREZ: What about with
15 any third parties?

16 CHIEF PRIVACY OFFICER GOLD: Surveillance
17 technology to third parties, not that I can think of.

18 DEPUTY COMMISSIONER GERBER: There may be
19 situations, just to be clear, depending on the
20 surveillance technology, there may be a vendor who
21 has access to information, right? And then that's
22 going to be governed by contract. Again, with
23 exhibit A which restricts their ability to use that
24 data.

2 CHIEF PRIVACY OFFICER GOLD: So, when we
3 have a technology where part of the use of the
4 technology requires it to interact with like the
5 vendor system, they are bound by what Commissioner
6 Gerber is talking about, New York City Appendix A
7 which has confidentiality provision within that, but
8 then that is also-- there might be further provisions
9 for data security. If it interacts with our cloud,
10 for example, there's a cloud writer that's a citywide
11 document that we could be using.

12 CHAIRPERSON GUTIÉRREZ: Sure.

13 CHIEF PRIVACY OFFICER GOLD: Or
14 identifying information writer or the privacy writer,
15 depends on what they're getting and how it's stored.

16 CHAIRPERSON GUTIÉRREZ: And who is--
17 what's the internal check on that? That there is--
18 like, this particular vendor is abiding by all that.
19 What does that look like?

20 CHIEF PRIVACY OFFICER GOLD: so, that
21 comes during while we're negotiating the terms of the
22 agreement to utilize the technology.

23 CHAIRPERSON GUTIÉRREZ: Okay.

24 CHIEF PRIVACY OFFICER GOLD: so, that's
25 assessed.

2 CHAIRPERSON GUTIÉRREZ: But while they're
3 accessing that information or during that duration is
4 there any additional-- is there any additional checks
5 after once the vendor has everything that they ask
6 for?

7 CHIEF PRIVACY OFFICER GOLD: I think that
8 would depend on the system and what audit processes
9 are in place for that specific technology.

10 CHAIRPERSON GUTIÉRREZ: Oh, I see. So
11 there's no like uniform kind of check on that once
12 they have the data that they are asking for.

13 CHIEF PRIVACY OFFICER GOLD: So, when
14 there's a cloud-- when there's-- so for example,
15 specifically when the cloud is being used, before we
16 can even give any data to a vendor with-- using their
17 cloud space as opposed to our cloud space, there's a
18 security check run on that. We have a Chief
19 Information Security Officer within ITB, Information
20 Technology Bureau, in NYPD and they check all of that
21 before we even are giving them anything.

22 CHAIRPERSON GUTIÉRREZ: Okay. I'm going
23 to-- I'll come back, but I'm going to switch gears to
24 OTI now. And can you just confirm if all-- does NYPD
25 handle all of its technology procurement in-house, or

2 does OTI ever have any input in the technology
3 procurements of NYPD?

4 CHIEF PRIVACY OFFICER FITZPATRICK: Thank
5 you for the question, Chair, and the opportunity to
6 participate in this important conversation today.
7 Again, I'm Mike Fitzpatrick, New York City's Chief
8 Privacy Officer. My office, the Office of
9 Information Privacy, became part of the Office of
10 Technology and Innovation when it was created by
11 Mayoral Executive Order Three of 2022.
12 Intentionally, bringing together the City's
13 technology and technology-related entities under one
14 common ecosystem and allowing for common touch-points
15 across subject matter expertise such as privacy,
16 information security, infrastructure management,
17 etcetera. From a procurement perspective, those are
18 responsibilities that are managed by others at the
19 Office of Technology and Innovation. However, my
20 understanding is that our procurement folks negotiate
21 citywide contracts that individuals' agencies are
22 capable of leveraging for their needs, most notably
23 to drive cost-efficiency, but my understanding as
24 well is that our agency does not-- is not involved in
25 any direct procurements for the Police Department.

2 But of course, I'll turn it over to my colleagues to
3 clarify if I've gotten that wrong.

4 CHAIRPERSON GUTIÉRREZ: Any response from
5 the agency?

6 DEPUTY COMMISSIONER GERBER: Chair, I just
7 wanted to clarify one point from before which I
8 think-- maybe just-- [inaudible] this, maybe not I'm
9 not sure. When we're talking about vendors having
10 access to data, we're not-- there's a not situation
11 where someone's coming to us and saying, "Hey, can
12 you give us this data." Right? We're talking about
13 in order to operationalize a particular surveillance
14 technology, it involves some third party vendor, and
15 necessarily in the nature of using that surveillance
16 technology, the vendor will by definition have access
17 to the data, and therefore we have to make sure it's
18 secure and not be used improperly. I just wanted to
19 be clear. This is not-- we're not talking about a
20 situation where-- you know, where we're just choosing
21 to give data to a third party. This is all within
22 the context of, alright, we have a surveillance
23 technology, we're operationalizing it. That involves
24 a vendor, and that can come up in various contexts,

1 COMMITTEE ON PUBLIC SAFETY WITH COMMITTEE ON TECHNOLOGY 40

2 and then how do we make sure the data is secure. I
3 just wanted that to be clear. That's all.

4 CHAIRPERSON GUTIÉRREZ: Okay, thank you.
5 I still have some follow-up questions, but thank you
6 for that clarity. I'm going to go back to OTI. So, I
7 guess the sense that I'm getting is that there is a
8 level of procurement involvement that OTI has, but it
9 sounds like PD for the most part has free reign to
10 kind of manage that system independently, regardless
11 if it's technology or surveillance specifically.

12 CHIEF PRIVACY OFFICER FITZPATRICK: So,
13 I'm not sure that I would characterize it as free
14 reign.

15 CHAIRPERSON GUTIÉRREZ: That's the way I
16 understood it. So, clarify, please.

17 CHIEF PRIVACY OFFICER FITZPATRICK: So,
18 again, as I understand it, and again, I'm happy to
19 bring questions back to the procurement folks who
20 specialize in this. The agency negotiates citywide
21 contracts for services. Again, notably to get the
22 most effective cost for the delivery of those
23 services, that individuals agencies are capable of
24 leveraging. So, I think for example, something as
25 basic as a cellphone plan. Rather than having each

1 COMMITTEE ON PUBLIC SAFETY WITH COMMITTEE ON TECHNOLOGY 41
2 individual agency contract for those services and
3 achieve different rates, the Office of Technology and
4 Innovation procurement will negotiate a common rate
5 to get the most effective price for the
6 Administration and the City.

7 CHAIRPERSON GUTIÉRREZ: Okay. So I guess
8 to that end, in procuring technology contracts, PD,
9 are there specific OTI stipulations that you are all
10 subject to around things like cyber security and data
11 management practices? How does that look like?

12 CHIEF PRIVACY OFFICER FITZPATRICK: I'm
13 happy to take this first. So again, as I mentioned,
14 with the consolidation of the City's technology-
15 related entities into the Office of Technology and
16 Innovation, we've brought together the City's subject
17 matter expertise and policy offices as it relates to
18 a number of different articles of which mine is
19 information privacy. For me, as Chief Privacy
20 Officer in the role of my office, we have the
21 responsibility of setting citywide privacy policies
22 that all agencies follow pursuant to the identifying
23 information law.

24 CHAIRPERSON GUTIÉRREZ: PD included?
25

2 CHIEF PRIVACY OFFICER FITZPATRICK: PD
3 included.

4 CHAIRPERSON GUTIÉRREZ: Okay. And is
5 there any-- and this also includes cyber security and
6 data management services?

7 CHIEF PRIVACY OFFICER FITZPATRICK: Cyber
8 security is the responsibility of our Office of Cyber
9 Command which provides that particular expertise.
10 But through that consolidation, for example, we've
11 actually been very well positioned to harmonize those
12 policy requirements across the City. So, for
13 example, the most recent revisions to our citywide
14 privacy policies that occurred earlier this year,
15 included such a harmonization by necessarily
16 integrating the City's cyber security policies with
17 direct links to them, recognizing the different
18 practice areas often overlap, but allowing for that
19 information to be available to agency employees in
20 one place.

21 CHAIRPERSON GUTIÉRREZ: Can you explain
22 how agencies follow this, these policies? Like what
23 is the checks? How are you all checking in with them
24 to ensure that these agencies-- the agencies are
25 following these policies?

2 CHIEF PRIVACY OFFICER FITZPATRICK:

3 Absolutely. So thank you for that question, Chair.

4 The identifying information which identifying
5 information law, rather, which is my area of concern,
6 naturally integrates a very strong governance regime
7 on a citywide level from agency operations as it
8 relates to identifying information. That law
9 requires every city agency to have a privacy officer
10 designated, and that privacy officer is intentionally
11 so empowered by the law to evaluate collections or
12 disclosures of identifying information by their
13 agency through the lens of legal requirement, as well
14 as the agency's overall mission or purpose.

15 CHAIRPERSON GUTIÉRREZ: And--

16 CHIEF PRIVACY OFFICER: [interposing]
17 Those-- oh, sorry.

18 CHAIRPERSON GUTIÉRREZ: No, no, I just--
19 does that happen on a-- like a consistent, like once
20 a year, once a quarter? How often does that need to
21 happen?

22 CHIEF PRIVACY OFFICER: So, those
23 evaluations on the agency level are occurring as
24 necessary by their privacy officer if, for example, a
25 new initiative is contemplated by an agency. That

2 would be something that should be-- that would
3 involve their privacy officer for consideration. An
4 additional element of the identifying information law
5 is the biannual requirement. Every two years, every
6 city agency does a review of its policies and
7 practices as it relates to identifying information.
8 Those reports-- we're actually approaching another
9 compliance cycle which will be due July of next year.
10 Those reports are submitted to the council, and kick
11 off another critically important element of the
12 identifying information law which is the review of
13 the City's Citywide Privacy Protection Committee of
14 those reports. That committee is defined with
15 particular agencies having a statutory seat at that
16 table, as well as the flexibility of the Mayor to add
17 additional agencies as they see fit. That committee
18 in reviewing those reports on a citywide level drives
19 toward the development of recommendations to the
20 Chief Privacy Officer on how citywide privacy policy
21 can be revised based upon the observations contained
22 within those reports. Those recommendations are
23 provided to the council as well as to me on October
24 of compliance years, and then formally transferring
25 the responsibility to me and my office in terms of

2 auctioning those recommendations. So, it's a very
3 important, and I think practice that the identifying
4 information law codified as it relates to that
5 biannual review recognizing privacy practices must
6 necessarily be considered periodically and evolve
7 over time.

8 CHAIRPERSON GUTIÉRREZ: Thank you. I'm
9 going to ask just two more questions and I have some
10 follow-up, but I definitely want to let my colleagues
11 ask a couple-- ask their questions. So I just have
12 two more before I pass it off. Can you share what
13 information was provided to OTI from PD related to
14 the POST Act in this past year?

15 CHIEF PRIVACY OFFICER FITZPATRICK: The--

16 CHAIRPERSON GUTIÉRREZ: [interposing] Or
17 detail which projects.

18 CHIEF PRIVACY OFFICER FITZPATRICK: So,
19 the POST Act does not include the Office of
20 Technology and Innovation, I would say. However--

21 CHAIRPERSON GUTIÉRREZ: [interposing] But
22 even in new procurement?

23 CHIEF PRIVACY OFFICER FITZPATRICK: Well-

24 -

2 CHAIRPERSON GUTIÉRREZ: [interposing]

3 So,-- okay, sorry, I'll let you finish. I apologize.

4 CHIEF PRIVACY OFFICER FITZPATRICK: So,
5 however, critically important, the identifying
6 information law to the extent that such technologies
7 involve the collection or disclosure of identifying
8 information, the identifying information law still
9 provides a governance regime.

10 CHAIRPERSON GUTIÉRREZ: Okay. I guess I'm
11 just trying to grapple. I know that-- I know that
12 Commissioner Fraser on a couple of instances has said
13 where funding requests go through OTI, but you're
14 saying not the case with PD and the POST Act in
15 purchasing of new surveillance equipment or
16 technology equipment?

17 CHIEF PRIVACY OFFICER FITZPATRICK: I can
18 only speak to that from a privacy perspective.
19 Again, there are others within the Office of
20 Technology and Innovation that have varying
21 responsibilities, again, through procurement. My
22 understanding is that the Office of Technology and
23 Innovation has not done individual procurements for
24 the Police Department as it relates to surveillance
25

2 technology, but if there are follow-up questions, I'm
3 happy to bring them back.

4 CHAIRPERSON GUTIÉRREZ: And can PD-- can
5 PD speak to that?

6 DEPUTY COMMISSIONER GERBER: I'm sorry to
7 which question?

8 CHAIRPERSON GUTIÉRREZ: With relation to
9 the POST Act and the integration of new technologies
10 and new equipment, is that something that you all for
11 the purpose of procurement, for example, work with
12 OTI on or no?

13 DEPUTY COMMISSIONER GERBER: Yeah, our
14 Chief Contracting Officer is here. I think he can
15 answer that question.

16 CHIEF CONTRACTING OFFICER MENDOZA: Could
17 you ask the question again?

18 CHAIRPERSON GUTIÉRREZ: Sure. So I guess--
19 - I've asked OTI, have the response, they're going to
20 get back to me, but I'm curious with relation to the
21 POST Act and any surveillance or technology projects
22 that PD is pursuing for the purpose of procurement,
23 for example, is there any communication that they
24 made to OTI, for example? Because the way I have
25 understood and the way that Commissioner Fraser has

2 testified in the past is obviously related-- anything
3 related-- under OTI, everything related to technology
4 from any agency sees OTI at some point. And so I'm
5 just trying to understand for the purpose of the POST
6 Act when that happens.

7 CHIEF CONTRACTING OFFICER MENDOZA: So,
8 it would depend on the specific procurement. Again,
9 OTI is not overseeing our procurement process.

10 CHAIRPERSON GUTIÉRREZ: Totally.

11 CHIEF CONTRACTING OFFICER MENDOZA: if
12 we're purchasing a type of technology, surveillance
13 technology, that may include like a cloud component,
14 there are certain standard writers that should be
15 included in the contract. If any changes are made to
16 those writers, sometimes we'll be asked to confirm
17 with OTI if they generally agree with--

18 CHAIRPERSON GUTIÉRREZ: [interposing] So,
19 it has happened?

20 CHIEF CONTRACTING OFFICER MENDOZA: Yes,
21 it's not a formal approval process, and it's really
22 related to specific elements of the procurement, not
23 like the scope of what we're procuring.

24 CHAIRPERSON GUTIÉRREZ: Okay. Okay, well
25 thank you. I'm going to pass it over to my

2 colleagues. I believe Council Member Cabán is first
3 up. Thank you.

4 COUNCIL MEMBER CABÁN: thank you. So, I
5 just want to ask some follow-up question on various
6 parts of your testimony throughout the afternoon. I
7 want to start by going back to the IUPs for a moment.
8 How does-- how different does a technology have to be
9 to receive its own IUP, and I want to give an example
10 here to hone in on, right? Like, you have a
11 different IUP for CCTV cameras and situational
12 cameras, right? They're both cameras, but why does
13 the autonomous robot or the Times Square robot, like
14 why does that not have its own camera?

15 DEPUTY COMMISSIONER GERBER: Its own IUP
16 you mean.

17 COUNCIL MEMBER CABÁN: Its own IUP, yeah.

18 DEPUTY COMMISSIONER GERBER: So, and I
19 appreciate the question. There is by definition,
20 [inaudible] there is line drawing that has to be
21 done. There's-- that--

22 COUNCIL MEMBER CABÁN: [interposing] How
23 are you drawing them? I want to know what's--

24 DEPUTY COMMISSIONER GERBER: [interposing]
25 Council Member, I'm answering your question.

2 COUNCIL MEMBER CABÁN: I only have
3 limited time, though, so I just want you go get
4 straight to the point.

5 DEPUTY COMMISSIONER GERBER: Alright,
6 I'll get right to it. To the extent, the nature of
7 the surveillance is fundamentally different, we're
8 going to do a separate IUP. So, for example, drones,
9 a great example. Drones, obviously, yes those have
10 cameras, but the nature of, you know, surveillance
11 that's done by drones is fundamentally different than
12 the nature of surveillance that's going to be done by
13 a situational awareness camera.

14 COUNCIL MEMBER CABÁN: so why doesn't the
15 autonomous robot have its own?

16 DEPUTY COMMISSIONER GERBER: Right, so
17 the autonomous robot is-- there's a camera on that
18 robot, and the nature of that surveillance is not
19 different than the nature of the surveillance that is
20 done by any other type of situational awareness
21 camera. The robot is different, but the nature of
22 that recording is not.

23 COUNCIL MEMBER CABÁN: But if-- I mean,
24 if the nature of the type of surveillance and
25 recording were not different, then why does-- why do

2 we have it? Why does it exist? Why is it like-- if
3 it wasn't substantially different, if it wasn't
4 expanding the capacity or filling a gap in the area,
5 then I would presume it would be superfluous. It
6 wouldn't be needed.

7 DEPUTY COMMISSIONER GERBER: No, there
8 are two different things going on. One is the nature
9 of a camera. The other is how a camera's being
10 deployed. So if we have a the night scope [sic] K5
11 in the Times Square subway station, having that
12 camera there and the robot sort of moving about,
13 providing sort of a 360 view, you know, that may have
14 efficiency and value, but the nature of the camera
15 itself, the nature of the surveillance that is
16 happening is not different.

17 COUNCIL MEMBER CABÁN: But you're saying
18 that the added value that it has in comparison to
19 other "situational cameras" to-- you're making the
20 determination is does not-- it does not rise to the
21 level of needing a separate IUP. That I don't agree
22 with and I'd be curious to know whether DOI agrees
23 with that. I'm going to move on. So you had
24 mentioned that you do share surveillance technology
25 with other federal agencies, correct?

2 DEPUTY COMMISSIONER GERBER: In the
3 course of criminal investigations--

4 COUNCIL MEMBER CABÁN: [interposing] Just
5 yes or no. Like--

6 DEPUTY COMMISSIONER GERBER: [interposing]
7 I'm answering your question. In the course of
8 criminal investigations, we share evidence with our
9 law enforcement partners, and that includes evidence
10 gained through the deployment of surveillance
11 technology, yes.

12 COUNCIL MEMBER CABÁN: But my specific
13 question was like, do you share with agencies like
14 the FBI?

15 DEPUTY COMMISSIONER GERBER: In the
16 course of investigations, yes.

17 COUNCIL MEMBER CABÁN: Okay, thank you.
18 And do you share with the Joint Terrorism Taskforce,
19 the Homeland Security Investigations Taskforce, high
20 intensity drug trafficking areas? Are those some of
21 the Departments that you share information with?

22 DEPUTY COMMISSIONER GERBER: In the course
23 of investigations, we definitely share with our law
24 enforcement partners, yes.

2 COUNCIL MEMBER CABÁN: And then you
3 testified that you don't share information with ICE,
4 correct?

5 DEPUTY COMMISSIONER GERBER: We do not
6 provide information to ICE, correct.

7 COUNCIL MEMBER CABÁN: So, but do you
8 share any surveillance technology data with other
9 agencies or third parties that then can-- may share
10 that data with ICE? So, for example, when you share
11 information with the FBI, do you prevent the FBI from
12 sharing that information from ICE-- sharing that
13 information with ICE?

14 DEPUTY COMMISSIONER GERBER: There is
15 absolutely no reason to think that in the course of a
16 criminal investigation into a particular criminal
17 organization or individuals, that the FBI would be
18 giving that information to ICE.

19 COUNCIL MEMBER CABÁN: That wasn't my
20 question. My question was, when you share
21 information with the FBI, do you prevent them from
22 sharing that information with ICE?

23 DEPUTY COMMISSIONER GERBER: That
24 information is to be used for the investigation at
25

2 issue. It is not-- as with any investigation,
3 they're investigation-specific. It would be--

4 COUNCIL MEMBER CABÁN: [interposing]

5 You're not--

6 DEPUTY COMMISSIONER GERBER: [interposing]

7 I am answering your question which is that we provide
8 it for that investigation.

9 COUNCIL MEMBER CABÁN: Yes, and when you
10 provide it to the FBI, yes or no, do you do anything,
11 are there any mechanisms in place to prevent them
12 from sharing that information with ICE?

13 DEPUTY COMMISSIONER GERBER: To the
14 extent there's a taskforce and there's an MOU for the
15 taskforce, that MOU may or may not govern how
16 information is being used in the course of taskforce
17 investigations. That is going to depend on the
18 particular taskforce and the nature of the MOU that
19 exists for that taskforce.

20 COUNCIL MEMBER CABÁN: So, if there's
21 information that you give to that-- may I have a few
22 more minutes please? If there's information that you
23 give to a taskforce or an agency in the MOU, is it
24 your standard practice to set an agreement that that
25 information will not then be passed off to ICE?

2 CHIEF PRIVACY OFFICER GOLD: The
3 information that we share through the course-- for
4 the taskforce is only to be used for taskforce
5 investigations only.

6 COUNCIL MEMBER CABÁN: And so do you
7 enforce that?

8 CHIEF PRIVACY OFFICER GOLD: That's an
9 operational enforcement, because the members of the
10 taskforce, whether federal or NYPD are still required
11 to follow their own confidentiality rules within
12 their agencies.

13 COUNCIL MEMBER CABÁN: Okay, but the
14 rules within that agency might be different than the
15 rules within this agency that is-- that exists in a
16 sanctuary city, correct?

17 CHIEF PRIVACY OFFICER: But to the extent
18 that they sign onto the MOU that requires them to
19 only use it-- use the information that they gain for
20 taskforce investigations. That's the security
21 measure.

22 COUNCIL MEMBER CABÁN: Okay. I'm going
23 to move on. I have two more questions. I want to be
24 respectful of my colleague's time, and thank you for
25 indulging me, Chairs. But the first is about

2 Clearview AI facial recognition. When you were using
3 that, who controlled the data? why were officers
4 using Clearview AI without any policy in place about
5 how that data was maintained, and who had access to
6 it? And then I just have one final question after
7 that.

8 DEPUTY COMMISSIONER GERBER: The
9 Department's policy is very clear. When using facial
10 recognition, the photo repository that is used is
11 arrest photos and parole photos. Absent authorization
12 from either the Chief of Detectives or the Deputy
13 Commissioner of Intelligence and Counterterrorism,
14 officers aren't-- detectives are not permitted to
15 conduct facial recognition outside of the universe I
16 just described. So whether it's Clearview or
17 anything else, you cannot go outside that photo
18 repository of arrests and parole photos absent
19 authorization from one of the individuals I just
20 mentioned. To the extent you don't have that
21 authorization, you absolutely cannot conduct facial
22 recognition using Clearview or any other facial
23 recognition system.

24 COUNCIL MEMBER CABÁN: Thank you.
25 Hopefully one of my colleagues follow up on that. My

2 final question is just-- you were part of, along with
3 other agencies, in agreement. So, the NYPD and the
4 DOI, the Comptroller, the Mayor's Office of Contract
5 Services, the Mayor's Office of Management and
6 Budget, the Law Department, you all had an agreement
7 to hide special expenses of budget contracts which
8 includes a lot of your surveillance contracts, and
9 then Comptroller Stringer withdrew from agreement
10 after the POST Act passed. Are the agencies still
11 abiding by that agreement to keep this info from the
12 public? Like, is everybody still a part of that
13 agreement? Is there a new agreement? That's my last
14 question.

15 DEPUTY COMMISSIONER GERBER: Council
16 Member, I do not accept the premise of your question,
17 and we are--

18 CHAIRPERSON HANKS: [interposing] Thank
19 you so much. We have to move onto--

20 DEPUTY COMMISSIONER GERBER: [interposing]
21 abiding--

22 CHAIRPERSON HANKS: the next Council
23 Member to ask a question I want to recognize Council
24 Member Brewer, and we're going to move on to Council
25 Member Joseph.

2 COUNCIL MEMBER JOSEPH: Thank you, good
3 afternoon. I wanted to talk about Digidogs. So, I
4 wanted to find out how many Digidogs did the NYPD
5 purchase.

6 UNIDENTIFIED: Yeah.

7 COUNCIL MEMBER JOSEPH: Does the NYPD
8 plan to purchase more Digidogs.

9 CHIEF MADDREY: Thank you for your
10 question, Council Member. How are you?

11 COUNCIL MEMBER JOSEPH: I'm good.

12 CHIEF MADDREY: Good. We've purchased
13 two Digidogs. At this time, we don't have any plans
14 to purchase any more.

15 COUNCIL MEMBER JOSEPH: According to
16 Politico, two Digidogs cost about \$750,000. Does
17 this contract include maintenance, annual software
18 update, patching mechanism, or other upkeep
19 procedures? Maintenance, are you going to maintain
20 it?

21 CHIEF MADDREY: The price that you quoted
22 is accurate. The full details of the contract I do
23 not have, but I can get.

24 COUNCIL MEMBER JOSEPH: You're going to
25 get that information for me.

2 CHIEF MADDREY: I can get that for you.

3 COUNCIL MEMBER JOSEPH: Because for
4 \$750,000 I hope somebody is taking care of that,
5 updating, the software, making sure it lasts. How
6 often have the Digidogs have been used since their
7 purchase?

8 CHIEF MADDREY: We deployed them five
9 times since we purchased them.

10 COUNCIL MEMBER JOSEPH: And what was the
11 reason for the deploy?

12 CHIEF MADDREY: They were deployed for
13 situation where people were armed with firearms,
14 barricaded in homes.

15 COUNCIL MEMBER JOSEPH: Was it helpful?

16 CHIEF MADDREY: Yes, it is helpful. It
17 is helpful. As the Chief of Department, my main
18 concern is making sure that not only do I keep my
19 officers safe, that I keep the public safe. Digidog
20 is a tool that helps us to go into a situation where
21 a person may be armed, and hopefully we have the
22 opportunity to see what the person has-- if they do
23 possess a weapon, alright? Instead of sending my
24 officers in there first, I can send the robot in
25 there, and I don't want anything to happen to the

2 robot, but if it does, you know, it is what it is. We
3 have to make sure our officers are safe, and we also
4 have to make sure the people we're trying to help are
5 safe. Earlier this year when we had the parking
6 garage that collapsed over here, it was through the
7 use of Digidog we were able to find unfortunately
8 someone who was in there buried. But Digidog was
9 able to go in there when police officers or
10 firefighters could not go in there.

11 COUNCIL MEMBER JOSEPH: Okay, thank you.

12 After introducing the Digidog and a K5, the Mayor
13 stated this is the beginning of a series of roll-
14 outs. Are we going-- we're going to do? So the
15 public safety-- in the statement it said, the public
16 safety has transformed itself. What other
17 technologies are in the pipeline for NYPD?

18 CHIEF MADDREY: Well, I think right now
19 we're looking at different technologies. The biggest
20 thing that we've been using with a lot of success are
21 the drones, the unmanned aerial systems. That's what
22 we're really using. We're really trying to learn
23 that technology better and expand that technology. I
24 have many, many events that I can discuss with using
25 the drones were extremely helpful. It helped public

2 safety. It helped police officer safety. So our
3 done technology is one the-- probably the biggest
4 thing that we're looking to expand on right now.
5 There's other things that are-- were being looked at.
6 We're always looking at new technology when it's
7 delivered to us, but nothing that we're really ready
8 to move on just yet.

9 COUNCIL MEMBER JOSEPH: Are you looking
10 into AI as part of your technology, and--

11 CHIEF MADDREY: AI is already out there.
12 It exists.

13 COUNCIL MEMBER JOSEPH: It's out there.
14 Are you training your officers to use AI for weapon
15 detection?

16 CHIEF MADDREY: We don't use AI in the
17 Department.

18 DEPUTY COMMISSIONER GERBER: And just to
19 be clear about that, you know, it really depends what
20 your question is. In terms of like some free-
21 standing AI training. We don't do that. There are
22 certain technologies we have where the sort of the
23 background to the technology is--

24 COUNCIL MEMBER JOSEPH: [interposing] Is
25 AI.

2 DEPUTY COMMISSIONER GERBER: AI, machine
3 learning based.

4 COUNCIL MEMBER JOSEPH: Correct.

5 DEPUTY COMMISSIONER GERBER: We have a few
6 things like that, but we don't have sort of a--
7 there's no-- I'm not aware of some like free-standing
8 AI initiative if that makes sense. But to your
9 point, there are a few surveillance technologies we
10 have where the-- there's sort of machine learning
11 that allows the technology to function, and that does
12 fall within the scope of AI.

13 COUNCIL MEMBER JOSEPH: And some of it
14 also AI where you can detect the weapon if somebody
15 pulls out a weapon in the surveillance part.

16 DEPUTY COMMISSIONER GERBER: We do not do
17 that. We don't have that.

18 COUNCIL MEMBER JOSEPH: You don't have
19 that.

20 DEPUTY COMMISSIONER GERBER: We certainly
21 don't use it. We certainly don't have the-- that is
22 not a technology that we have deployed.

23 COUNCIL MEMBER JOSEPH: And how often are
24 your officers trained on this new technology once it
25 comes into use?

2 CHIEF MADDREY: It's a rigorous process.
3 When we have-- when we obtain new technology, it
4 doesn't go to the masses within the Department. It's
5 usually within our Technical Assistance or Response
6 Unit, commonly known as TARU. We usually-- our TARU
7 officers who are trained in technology, in various
8 forms of technology. We usually allow them to use it
9 first through a pilot phase, a test phase. Then if
10 it's something that works, then we'll expand it.

11 COUNCIL MEMBER JOSEPH: And there's been
12 training-- and it's been helpful the way you're
13 training your small units.

14 CHIEF MADDREY: Yes.

15 COUNCIL MEMBER JOSEPH: Thank you.

16 CHAIRPERSON HANKS: Council Member
17 Holden?

18 COUNCIL MEMBER HOLDEN: Thank you,
19 Chairs. A question on-- I guess for Deputy
20 Commissioner Gerber regarding the facial recognition
21 software, the improvements we've seen over the past
22 few years, because I hear a lot of, you know,
23 comments that it's not accurate, but it has improved
24 immensely from my research over the years. Can you
25 talk to that?

2 DEPUTY COMMISSIONER GERBER: Yeah, no, I
3 think that's exactly right. I think what you've seen
4 over the past few years, and there's been, you know,
5 academic work on this, scholarly work on this, that
6 really over the past few years, the accuracy of the
7 facial recognition software, you know, has improved
8 significantly. And you know, so we use a software
9 that has algorithms that have been reviewed by NIST,
10 National Institute of Standards and Technology. And
11 to your point, the technology, its accuracy has
12 improved very significantly I'd say over the past,
13 you know, half decade.

14 COUNCIL MEMBER HOLDEN: Were the-- could
15 you speak to the accuracy, though? Like what
16 percentage is, like, that comes up as an error in
17 certain software? Do you have those figures?

18 DEPUTY COMMISSIONER GERBER: That I do not
19 have here.

20 COUNCIL MEMBER HOLDEN: Okay, because
21 there's a lot of even businesses that have invested
22 in that to protect their property and to protect
23 their businesses. And it seems, you know, when I was
24 speaking to some of the business groups they were
25 saying that would actually disable many of the stores

2 from even-- or at least prevent them from operating
3 normally.

4 DEPUTY COMMISSIONER GERBER: One thing I
5 do want to emphasize is that when we talk about using
6 facial recognition technology, we are talking about
7 having multiple individuals reviewing that output and
8 reviewing the possibility of a potential match before
9 anything is provided to a detective.

10 COUNCIL MEMBER HOLDEN: So there's quite
11 a debate on that. They talk amongst themselves. Is
12 this the same guy? Is that-- that kind of thing, or?

13 DEPUTY COMMISSIONER GERBER: Right, so
14 you'll have an initial-- if a case detective requests
15 that facial, you know,-- a case detective submits an
16 image for facial recognition use. That image may or
17 may not be useable for facial recognition. It's
18 really going to depend. So sometimes, you know, a
19 photo is provided and it's rejected, because we can't
20 use it. If it is usable, you'll have an initial
21 detective who does this work who reviewed the output.
22 If that detective identifies a potential match, if
23 that happens, a second detective will also review to
24 see if he or she agrees on the potential match, and
25 then a supervisor will also review. And only if

2 there is complete agreement between the first
3 detective, the second detective and a supervisor,
4 will that be flagged for the case detective as a
5 potential match. So we have a lot of-- I think it's
6 very important that yes, there is of course, this
7 important technology that we're using, but there also
8 is-- there are substantial human checks in this
9 process, multiple human checks, and just to
10 emphasize, even when it's a potential match, it's
11 just a lead. That's all it is. It is not basis for
12 a probable cause.

13 COUNCIL MEMBER HOLDEN: It's a tool.

14 It's a tool, and-- but it does catch a lot of the bad
15 guys, I would say.

16 DEPUTY COMMISSIONER GERBER: Exactly. It
17 is--

18 COUNCIL MEMBER HOLDEN: [interposing] You
19 look at once we have a photo of the individual who
20 attacked a woman, let's say on the subway, once we
21 get that, many times that person is arrested. So, it
22 is working, and to eliminate that tool would be a
23 problem, especially with a smaller police force and
24 less detect-- I have half the amount of detectives in
25 my precinct that I use to have just a few years ago.

2 And so I can see it-- if we're not using technology
3 in the right way, obviously-- if we're not-- if we're
4 prohibited from using it, period, certain technology,
5 that's going to hurt us with public safety. I guess
6 the Chief can speak to that.

7 CHIEF MADDREY: You're absolutely right,
8 Council Member. We don't want to lose this
9 technology, and as the Commissioner said, the facial
10 identification just provides a lead. It-- from there
11 our detectives have to go out and do some good old
12 fashion detective work, knock on doors, use other
13 technology to verify that match, if the person they
14 believe it is, is that person, and if that person was
15 even in the position to do that crime. So it's just
16 a lead. It's a very helpful lead, something that
17 this department relies on, and it helps to solve
18 crime.

19 COUNCIL MEMBER HOLDEN: and that's why
20 the police force exist first of all, and public
21 safety. Let me just ask one other question. Deputy
22 Commissioner Gerber, you said you don't share
23 information with ICE at all.

24 DEPUTY COMMISSIONER GERBER: We are not
25 permitted to do anything basically in the world of

2 civil immigration enforcement. We're not allowed to
3 do that.

4 COUNCIL MEMBER HOLDEN: No, but well,
5 let's say there are two million people now on the
6 terror watch list, you know that? There's two
7 million people. It's the latest news that we have,
8 two million. So let's say your facial recognition
9 comes up with somebody and it pings on the fact that
10 this guy is on the terror watch list. Do you just go
11 to the FBI, or you won't--

12 DEPUTY COMMISSIONER GERBER: [interposing]
13 So, obviously, if--

14 COUNCIL MEMBER HOLDEN: [interposing] Do
15 you go to ICE?

16 DEPUTY COMMISSIONER GERBER: As a matter
17 of a criminal investigation we go to-- we have
18 various law partners, law enforcement partners, but
19 whatever else we're doing in the criminal realm, we
20 are not permitted to use Department resources,
21 Department information in connection with civil
22 immigration enforcement.

23 COUNCIL MEMBER HOLDEN: No, but I'm
24 talking about criminal. If--

2 DEPUTY COMMISSIONER GERBER: [interposing]
3 Right.

4 COUNCIL MEMBER HOLDEN: If somebody comes
5 in and he appears on the terror watch list and you
6 have a match. You notify ICE, then?

7 DEPUTY COMMISSIONER GERBER: We're going
8 to notify law enforcement partners in connection--

9 COUNCIL MEMBER HOLDEN: [interposing]
10 Right.

11 DEPUTY COMMISSIONER GERBER: with
12 potentially a criminal investigation, obviously.

13 COUNCIL MEMBER HOLDEN: Because I lived--
14 and most of us have lived through 9/11. We know why
15 customs enforcement was created, so that we could
16 communicate with agencies. So, not to communicate
17 with somebody who matches the terror watch list would
18 be ridiculous.

19 DEPUTY COMMISSIONER GERBER: Just to be
20 clear, the terror watch list is not part of our
21 facial recognition repository. I think it's
22 important just so the record is crystal clear, right?
23 Our facial recognition system, again, is off of
24 arrest photos and parole photos. It does not include
25

2 photos off of the terror watch list. That's totally
3 separate. And again--

4 COUNCIL MEMBER HOLDEN: [interposing] I
5 would say why not, but I just-- you know, that's me.

6 CHAIRPERSON HANKS: Thank you.

7 COUNCIL MEMBER HOLDEN: Thank you.

8 CHAIRPERSON HANKS: Thank you, Council
9 Member. Council Member Stevens?

10 COUNCIL MEMBER STEVENS: Hi, good
11 afternoon. I just wanted to just make sure and have a
12 couple of points, because when we talk about terror
13 watch lists and things like that, we have to be
14 careful about that because Nelson Mandela was on a
15 terrorist watch list for a number of years, and he
16 was a great man, and so obviously those things come
17 with biases, and because humans are always in charge
18 they also come with biases. So, it should be a tool,
19 but we also need to recognize the racial implications
20 that those come with, and so I think we need to be--
21 make sure that that needs to also be said. And also
22 just talking about technology, and I think that we
23 should be moving in a direction of technology and the
24 Police Department should be using those things, but
25 again, because of the relationship that they have

2 with certain communities, especially the black,
3 brown, Latino, and Muslims, this is why it is
4 becoming an issue because the mistrust is there, and
5 it hasn't been built, and so when we have these
6 things coming up, these issues, we're going to be
7 suspicious of it because we are not doing the work of
8 actually building these relationship and trust in all
9 communities. So I do think it's a lot easier for
10 other folks to lean into some of these things in an
11 easier way, because they're not discriminated against
12 continuously. But my question is, the Office of
13 Inspector General released a report on criminal group
14 database that stated that 99 percent of the
15 individuals found on the database were black or
16 Latino. How do you explain the huge racial
17 disparities found in these surveillance databases?

18 DEPUTY COMMISSIONER GERBER: I'll start
19 and then turn it over to the Chief. I do think it's
20 important in responding to your question, part of the
21 response, I think it is important to emphasize that
22 that report which was, you know, exhaustive found no
23 evidence that inclusion in the criminal group
24 database caused harm to an individual or group of
25 individuals.

2 COUNCIL MEMBER STEVENS: That's you
3 making that assumption. The people that's on the
4 list might speak otherwise, but continue.

5 DEPUTY COMMISSIONER GERBER: I'm just
6 quoting form the report.

7 COUNCIL MEMBER STEVENS: I know, but I'm
8 just saying.

9 DEPUTY COMMISSIONER GERBER: It's DOI's
10 report. And they did not find any evidence of a
11 relationship between inclusion in the database and
12 any individual adverse outcomes. Again, that's the
13 DOI report speaking, not me. I think that's
14 important to say on the record.

15 COUNCIL MEMBER STEVENS: And even quoting
16 that means if it doesn't do anything, then why do we
17 have it.

18 DEPUTY COMMISSIONER GERBER: No, no, so--

19 COUNCIL MEMBER STEVENS: [interposing]
20 Because you quoted the report, right?

21 DEPUTY COMMISSIONER GERBER: Yes.

22 COUNCIL MEMBER STEVENS: So, we going to
23 quote the report and from the report that you just
24 quoted to try to say that it's not being used, then
25 why do we have it, then?

2 DEPUTY COMMISSIONER GERBER: No, no, it
3 is used as an investigative tool. I just think it's
4 important to emphasize that that information is not
5 being provided, for example, to-- it's not part of
6 one's criminal history. It's not provided to
7 potential employers. It's not provided in connection
8 with housing. I just--

9 COUNCIL MEMBER STEVENS: [interposing]
10 Then why is 99 percent of it black and Latino.

11 CHIEF MADDREY: Council Member, I think
12 when we just look at what's going on in our
13 communities, when you look at a lot of the gang and
14 the crew activities, a lot of--

15 COUNCIL MEMBER STEVENS: [interposing]
16 They're not just black and brown.

17 CHIEF MADDREY: A lot of it is based in a
18 lot of our communities in Brownsville, in--

19 COUNCIL MEMBER STEVENS: [interposing] I'm
20 disappointed that you as a black man would even say
21 that.

22 CHIEF MADDREY: But you're taking it--

23 COUNCIL MEMBER STEVENS: [interposing]
24 Every racial group has gangs.

2 CHIEF MADDREY: You're taking it the
3 wrong way. We're talking about just the sheer
4 numbers. I'm not saying it doesn't exist in other
5 neighborhoods, but I'm just saying in our particular
6 neighborhood, we do see a number of gangs and crews.
7 This is an internal intelligence piece. As the
8 Commissioner said, we don't share with people, it's
9 all internal information. There's a series of steps
10 that we go through before we put anybody on there,
11 and there's a series of steps that we go through--

12 COUNCIL MEMBER STEVENS: [interposing] so
13 then what are the tools that you're using to
14 surveillance people who are not black and brown?
15 Because if you're going to say that in these
16 communities, there are high numbers of gangs. That
17 means that okay, great, and we know that there other
18 communities that have gangs and do criminal
19 activities. Where's their database? Where's their
20 use for investigations? Where is that information
21 being kept? Because if it's one specific group, it
22 seems like they're being targeted.

23 CHIEF MADDREY: Well, we have an
24 intelligence division that keeps different
25

2 information on different groups. I mean, there's
3 information all kinds of criminal groups.

4 COUNCIL MEMBER STEVENS: Could you give
5 us information about where those other databases is
6 on the other groups? Because maybe that would
7 probably help with some of it, but when we have a
8 database that is 99 percent black and Latino, that's
9 a concern and red flag for me. And if it's not for
10 everyone sitting up here, that's a problem for me,
11 because that means that you're watching a certain
12 group of people while others aren't getting the same
13 level of scrutiny. And even when we talk about the
14 [inaudible] to get on there, it's very subjective.

15 CHIEF MADDREY: The way you get on there
16 is not subjective. A lot of it has to do with self-
17 admission. A lot of it has to do with self-
18 admission, and a lot of young people that we bring
19 and they do self-admit yes, I'm a part of this. They
20 don't hide it.

21 COUNCIL MEMBER STEVENS: So, alright--

22 CHIEF MADDREY: [interposing] But just to
23 go back--

24 COUNCIL MEMBER STEVENS: [interposing]
25 You know I know those criteria.

2 CHIEF MADDREY: No, just to go back to
3 your point. We have organized crimes groups, we have
4 database and information on organized crime, people
5 who in there and they don't look like people from our
6 communities. Some do, some don't. We have different
7 databases. I understand that the crew, gang crew
8 database has been a very-- a subject that's, you
9 know, resonated poorly throughout our communities,
10 because yes, there have been young people who have
11 been put on there and we've gone through steps to
12 remove them and as well as [inaudible]--

13 COUNCIL MEMBER STEVENS: [interposing] And
14 part of the problem is some young people don't even
15 know that they're on the database. So, listen, you
16 know this is one of the areas I actually know a lot
17 about. So like, let's not pretend like you don't
18 know that you're on there. It's a secret. You don't
19 know how to get off of there. The steps to FOIL to
20 do it is very difficult and arduous, but what I'm
21 saying is that I'm going to wrap up because I know
22 there's other people in regards on the time limit.
23 It is a problem that 99-- I'm going to say this
24 again, 99 percent of those folks on there are black
25 and brown which is why-- every reason why they're

2 pushing back on any new technology, surveillance,
3 because this is another reason why people don't trust
4 the work that is being done. This is a reason, I'm
5 telling you. Like, we don't feel safe, because why
6 would you have a database that literally racially
7 profiling? But this is-- I'm telling you, we got to
8 get to a place where everyone feels safe and everyone
9 feels like they're being included, and that's just
10 not the case and this is an example of that. So
11 thank you.

12 CHAIRPERSON HANKS: Council Member
13 Stevens-- Council Member Paladino?

14 COUNCIL MEMBER PALADINO: Good afternoon.
15 I have a couple of simple questions. given the
16 NYPD's opposition to the POST Act, can the Department
17 elaborate on the challenges it faces in balancing
18 transparency with the need to protect sensitive
19 operational details from potential criminal
20 exploitation?

21 DEPUTY COMMISSIONER GERBER: I'll take
22 that. This is-- relates to question that Chair Hanks
23 asked earlier. When we are do-- when we did the IUPs
24 initially, and then we do the addendums to the IUP,
25 yeah, we have to follow the law. We have to make

2 sure we're making the requisite disclosures
3 consistent with the Act. We do have to be careful
4 not to compromise public safety, and we would not
5 want to, for example, put our undercover's at risk.
6 We would not want to take steps that would hurt
7 public safety efforts. I think, you know, the way
8 we've-- the way the POST Act is working, I think--
9 we, consistent with the law, have been able to strike
10 that balance. Again, I do have real concerns that
11 Intro 1207 shifts that balance or at least risks
12 shifting that balance in a way that will compromise
13 public safety efforts.

14 COUNCIL MEMBER PALADINO: Because the
15 NYPD was against the POST Act back in 2020.

16 DEPUTY COMMISSIONER GERBER: We were.

17 COUNCIL MEMBER PALADINO: Right, okay.
18 One of the other questions I had was can you
19 elaborate on how disclosure of surveillance
20 capabilities as required by the POST Act could
21 specifically endanger your undercover officers and
22 compromise their safety?

23 DEPUTY COMMISSIONER GERBER: Yeah, this
24 goes to the hardware point. So we have an IUP for
25 each type of surveillance technology. We don't break

2 it down by each type of hardware, and that plays out
3 in a lot of different ways, and if we had to do it,
4 you know, hardware by hardware, there'll be a lot of
5 problems with that. Some of them administerability
6 [sic], some of them I think actually confusion of the
7 public, but it actually goes to this point about
8 undercovers. It is one thing to say publicly we, you
9 know, have under-- we have covert recording devices,
10 covert video recording devices, covert audio
11 recording devices. It's one thing to explain that at
12 a certain level of generality, to explain the rules,
13 laws, procedures that govern those investigative
14 tools. It would be something else entirely if we had
15 to do a new IUP for each type of hardware in which a
16 surveillance technology is deployed. That would be
17 for our undercovers very dangerous.

18 COUNCIL MEMBER PALADINO: [inaudible] I
19 got it. I'm on. Okay. How does the NYPD assess the
20 impact of POST Act-- of the POST Act on its
21 counterterrorism efforts? Are the concerns of that
22 Act, and could they inadvertently aid terrorist
23 organizations by revealing these surveillance
24 tactics?

1 COMMITTEE ON PUBLIC SAFETY WITH COMMITTEE ON TECHNOLOGY 80

2 DEPUTY COMMISSIONER GERBER: so, I think
3 in terms of where we are now, you know, I think-- I
4 do not think that the POST Act has compromised those
5 efforts. I would be concerned about changes to the
6 language of the POST Act that would require, again,
7 IUPs on a hardware by hardware basis or in a more
8 granular way, I think raises the types of concerns.

9 COUNCIL MEMBER PALADINO: Thank you very
10 much.

11 CHAIRPERSON HANKS: Thank you so much,
12 Council Member Paladino. Abreu, Council Member
13 Abreu?

14 COUNCIL MEMBER ABREU: Thank you, Chairs.
15 I have a question on Digidogs. Where do they live?

16 CHIEF MADDREY: Where do they live?

17 COUNCIL MEMBER ABREU: Yeah, where do the
18 Digidogs live?

19 CHIEF MADDREY: They're at our TARU base.

20 COUNCIL MEMBER ABREU: Okay, where's
21 that?

22 CHIEF MADDREY: in Queens.

23 COUNCIL MEMBER ABREU: In Queens.

24 CHIEF MADDREY: By the Whitestone Bridge.

25

2 COUNCIL MEMBER ABREU: I have a question
3 in regards to the police-involved shooting earlier
4 this week. Were Digidogs deployed there?

5 CHIEF MADDREY: We had Digidog at the
6 scene. Digidog was--

7 COUNCIL MEMBER ABREU: [interposing]
8 Sorry, one question-- one second. I want to be able
9 to see you. Go ahead.

10 CHIEF MADDREY: Digidog was there.
11 Digidog was actually in the process of being
12 deployed, but we used the avatar first, and then
13 that's when things, you know, it got-- became
14 chaotic, and that's when the gunfire started.

15 COUNCIL MEMBER ABREU: Got it. So
16 Digidog was not used at that?

17 CHIEF MADDREY: Yeah, we didn't-- we
18 deployed some other forms of technology first. We
19 had Digidog there. We were ready to deploy it, but
20 that's-- the gunfire started before we had a chance
21 to use Digidog.

22 COUNCIL MEMBER ABREU: And is it because
23 Digidog was maybe too far away, or just the timing of
24 it didn't work out? Because I do know-- you
25 mentioned in your testimony earlier that Digidogs

2 would be deployed in situations where people are
3 armed. I want to make sure that we're, of course,
4 maximizing the use of Digidog.

5 CHIEF MADDREY: Absolutely, but we do
6 have other forms of technology that can also do the
7 same thing that Digidog can do. We sent a scout in
8 first. A scout is like a small ball that goes in
9 there. It has a camera. The person in there was able
10 to immobilize the scout by throwing something on it.
11 We actually used a drone first, a small drone. The
12 person took a broom and swatted the drone down.

13 COUNCIL MEMBER ABREU: That's right. I
14 read that.

15 CHIEF MADDREY: Destroyed the drone.
16 Then we sent the avatar in, which is basically a
17 camera that's on wheels. It's like a camera-- a set
18 of wheels. The camera is a pole camera. We sent
19 that in, and emergency service kind of walking behind
20 it because they were trying to close the distance
21 between themselves and the suspect. That's when the
22 suspect emerged from the bathroom door and started
23 firing.

24 COUNCIL MEMBER ABREU: Thanks for that,
25 Chief. You also mentioned earlier in your testimony

2 that there were five situations where Digidog has
3 been deployed. One of them was the garage collapse.
4 Can you-- to the extent you have those, can you speak
5 to the other four situations that they were used for?

6 CHIEF MADDREY: I can't speak to all of
7 them. I can speak to two that are-- that I was a
8 little bit more-- you know, I was at the scene of.
9 One was-- about a month ago we had a situation over
10 in Astoria where a resident of building shot his
11 super, and then he ran inside and barricaded himself
12 inside. We were able to use Digidog, and the reason
13 we were able to use-- Digidog has the ability to walk
14 upstairs. So we used Digidog at that location. And
15 then we had another situation where there was a
16 person-- there was an emotionally disturbed person
17 who was-- we couldn't locate him in a building. So
18 we used Digidog to walk up and down the building and
19 we found him on the roof.

20 COUNCIL MEMBER ABREU: And so it seems it
21 was helpful for--

22 CHIEF MADDREY: [interposing] Absolutely.
23 We were able to use Digidog. We found him on the
24 roof. We were able to bring him-- you know, put him
25 in custody with no problem. So definitely helpful.

2 The other situation where we had Digidog and Digidog
3 went up there. Digidog was able to go up there, do
4 some surveillance for us, but eventually emergency
5 service had to move in a little closer. When we
6 moved in a little closer, the suspect shot himself.

7 COUNCIL MEMBER ABREU: Thank you. And
8 since I have one minute I just want to quickly pivot
9 to drones. Hopefully my colleagues can ask further
10 questions on drones. Who makes the decision about
11 how drones can be deployed, and where is drone-
12 recorded data stored?

13 CHIEF MADDREY: The decision comes from
14 me, one of my designees. It's usually the Chief of
15 Patrol, my Chief of Staff, or Chief of Special
16 Operations. What we do with the drone, we just--
17 basically right now we're still developing the whole
18 process, but we just take some notes of when we
19 deploy the drones if they was useful for what we
20 needed it for, and that's what we're doing right now.
21 Of course, we're going to improve that.

22 COUNCIL MEMBER ABREU: And what's the
23 done-- what are drones primarily used for?

24 CHIEF MADDREY: It's used really for
25 large scale events. We've used them with success at

2 large scale events. Electric Zoo that happened late
3 in the summer where about a thousand people crashed
4 the gates because there was a discrepancy with the
5 tickets. We were making the decision to close the
6 place down because we thought it was over-crowded. We
7 were able to put the drone up. We were able to get
8 an aerial view of the park, and we realized that the
9 place wasn't overcrowded, so we didn't have to create
10 a situation now where we're telling thousands of
11 people the event's over. We knew it was safe in
12 there, and we allowed the event to continue. Union
13 Square over the summer a bunch of young people
14 converged down there, you know, believing that they
15 were going to receive some gifts. I was there
16 personally on the scene and I couldn't gauge how many
17 kids were out there. Once we put the drone up there,
18 we realized we had up to 5-6,000 young people out
19 there, where from my vantage point it maybe looked
20 like a 1,000 or 1,500. So, again, very helpful. We
21 realized we had more young people out there than, you
22 know, we could handle at that moment. We had to
23 bring additional resources there, and we had to
24 figure out how to get them out which we were able to
25 do.

2 COUNCIL MEMBER ABREU: Thank you so much.
3 Appreciate it.

4 CHAIRPERSON HANKS: Thank you. Council
5 Member Brewer?

6 COUNCIL MEMBER BREWER: Thank you. Some
7 of my questions, because I was late, I had another
8 event. Might be for the next session. But I'm
9 always interested in the contracts, and obviously for
10 those drones, it's cyber security. I just want to
11 know, do you handle this in-house? Do you have-- how
12 many contracts do you have? How do you work with
13 Commissioner Fraser, etcetera? How do you put
14 together this procurement for technology?

15 CHIEF PRIVACY OFFICER FITZPATRICK: Thank
16 you for the question, Council Member. I'm Mike
17 Fitzpatrick, New York City's Chief Privacy Officer.
18 My office, the Office of Information Privacy is part
19 of OTI. I know you came in late, I just wanted you
20 know--

21 COUNCIL MEMBER BREWER: [interposing]
22 Well, I appreciate that. Thank you.

23 CHIEF PRIVACY OFFICER FITZPATRICK: So,
24 from a contracting perspective, in my role as the
25 Chief Privacy Officer, I have the responsibility of

2 providing agencies with standardized terms to support
3 data protection pursuant to our local identifying
4 information law. Those terms are part of citywide
5 privacy policy, and our agency privacy officers look
6 to those terms to support their agency negotiation of
7 contracts. Our policies provide that most notably, I
8 think, that when sensitive identifying information is
9 at issue, that is information that carries an
10 increased risk of harm to a particular individual,
11 that is a must-attach situation for a very specific
12 set of terms. And again, notably earlier this year,
13 pursuant to our latest revision to citywide privacy
14 policy we included an additional requirement that
15 those-- that contracting language cannot be changed,
16 without the express authorization of the Chief
17 privacy officer to add an additional control and
18 support for other data protection and privacy
19 protection at the agency level. So I'll answer that
20 from the policy perspective, and I'll turn it over to
21 my colleagues to speak to the Department's practices.

22 COUNCIL MEMBER BREWER: That's helpful.

23 DEPUTY COMMISSIONER GERBER: So, yeah, I
24 can speak to that. So, we obviously have internal
25 process review for any type of contracts that we

2 purchase. Obviously, the value of the contract, the
3 type of procurement that we're doing, the type of
4 surveillance technology we might be procuring will
5 have different types of steps of review to make sure
6 that the appropriate clauses and terms are included
7 in the agreement. In addition to that there's
8 obviously multiple levels of oversight review. When
9 we put together our contract after internal review by
10 our legal teams, which also goes to the New York City
11 Law Department who also does an additional layer of
12 review. I mentioned before that, you know,
13 occasionally we're asked if, you know, if we've made
14 changes to some of the agreements that are provided
15 by OTI, if OTI has concurred with any changes that
16 we've made, that usually happens through the Law
17 Department review process. So, again, multiple
18 layers internally as well as oversight review so that
19 all appropriate parties are informed of whatever type
20 of contract, and if there's any privacy concerns,
21 that they're addressed.

22 COUNCIL MEMBER BREWER: And it sounds
23 like it hasn't breached at all, in the sense that you
24 keep the information and that this contracting
25 process is working in terms of information not

2 getting to the private hands where it should not be.
3 Sounds right?

4 DEPUTY COMMISSIONER GERBER: To my
5 knowledge, yes.

6 COUNCIL MEMBER BREWER: Okay, do we have
7 some sense, because a lot of this has to be
8 contracted out, obviously-- do we have some sense
9 generally for NYPD how many contracts are let for
10 technology surveillance, etcetera? I mean, I know
11 it's a very broad question, I know that. But do you
12 have some sense on what the dollar figure is?

13 DEPUTY COMMISSIONER GERBER: I think we
14 do have some dollar figures that we can provide, and
15 I'll double-check to make sure we have them. We do
16 about anywhere from 2,500 to 3,000 individual
17 purchases, right? Those can be small contracts.
18 Those can be large contracts.

19 COUNCIL MEMBER BREWER: Per year is what
20 you're saying.

21 DEPUTY COMMISSIONER GERBER: Correct. So
22 again, you know, I don't have an exact figure for you
23 and how many of those things relate to surveillance
24 technology. I think we have some rough numbers of
25 spending regarding surveillance technology. I think

1 COMMITTEE ON PUBLIC SAFETY WITH COMMITTEE ON TECHNOLOGY 90
2 it's in the realm of 120 million dollars per year for
3 surveillance technology that's covered under the POST
4 Act.

5 COUNCIL MEMBER BREWER: Okay. The reason
6 I also ask is I know a bit about technology in my
7 past. It's always concerning to me that when you
8 contract out, which has to happen, then you don't
9 have the intellectual property internally, and when
10 that company contract end, sometimes so does the
11 information. Is that something that you're aware of
12 and deal with, or that's not an issue?

13 DEPUTY COMMISSIONER GERBER: I don't
14 think so. I mean, I believe our agreements contain
15 very specific language that any IUP created through
16 those contracts is retained by the City of New York.
17 So, I believe they would be in breach of contract if
18 they took any information from that engagement and
19 then used it elsewhere.

20 COUNCIL MEMBER BREWER: Okay. Thank you,
21 Madam Chair.

22 CHAIRPERSON HANKS: Thank you so much. I
23 just have a few questions, and I thank all my
24 colleagues for those great questions, and kind of
25 expanding on the questions from Council Member

1
2 Stevens. When it comes to the technology-- and there
3 are a lot of things that have been written about
4 coded bias. Is there any potential-- we know this,
5 but for racial biases and the underlying technologies
6 of certain surveillance utilized by NYPD, and if so,
7 does the Department mitigate that bias when using the
8 technology?

9 DEPUTY COMMISSIONER GERBER: So, I'll
10 start with that. I think one concern, for example,
11 that's been raised over the years is that sort of
12 bias in the facial recognition space. I do think-- I
13 do think that those concerns are much less now than
14 they were say five or ten years ago. I do think the
15 technology has gotten better, and that risk of bias
16 inherent in the technology has diminished. I also
17 think that the crucial point, again, is that we're
18 not just blindly, you know, following some output
19 from some facial recognition algorithm. That is the
20 starting point of a process that then goes to
21 multiple points of human review. A first detective,
22 a second detective, and a supervisor, and only if all
23 those three are in concurrence, only then does it get
24 passed along as a lead to the case detective. So I
25 do think that that's an example of a situation of

2 which the human element on top of the technology, you
3 know, should have a mitigating effect in terms of the
4 issue that you're raising.

5 CHAIRPERSON HANKS: Thank you so much.

6 So, do you have any internal audits on this use of
7 technology when it comes to the surveillance audits?
8 I think you started by saying you have, you know, a
9 detective, a process, but then you know, things are
10 changing rapidly. Is there a space where there's an
11 audit process where it's quarterly, yearly-- you
12 know, there is a human component to this. what I
13 think the question is surrounding on is there a
14 compliance, an audit as time goes on to make sure--
15 recalibrate, I guess the word is, to make sure that
16 the technology that even the officers who are looking
17 at this are in the right and correct head space.

18 DEPUTY COMMISSIONER GERBER: So, with
19 regard to any surveillance technology there's always--
20 - you know sometimes audits can be ordered in a
21 variety of contexts for a variety of reasons. I
22 think the question that you're asking is about is
23 there some regular audit that is done in terms of the
24 facial recognition procedures, I'm actually not sure
25 about that. I'm not aware of that, but it's possible

2 that I just don't know about it, but I'm not aware of
3 that.

4 CHAIRPERSON HANKS: And finally, before I
5 pass it along to my Chair, and I also just want to
6 thank you all for your testimony and answering our
7 questions to the best of your ability. We had a-- in
8 Staten Island Northshore, we had a summer stage
9 concert, and I noticed that there were drones being
10 used. It was probably one of the first events in my
11 district where it was 5,000+. It was-- we considered
12 it an incredible event. Is there a mechanism in
13 which we're told that if we have an event, especially
14 as a Council Member, people who are-- you know, we're
15 funding these events. It's our names on the flyers
16 and the outreach. Is there any way or is there any
17 mechanism in which you are letting us know as Council
18 Members or as event organizers, because to your point
19 they were very helpful to you. I just wish you took
20 better pictures. But, you know, we just wanted to
21 kind of get an idea that-- I didn't know that it was
22 being used, and I thought it was media. I thought it
23 was, you know, a newspaper. How do we know which
24 drone is being used for what purpose and what agency?

2 CHIEF MADDREY: We can definitely build
3 that mechanism in. I don't believe we have one right
4 now, but that's something that's a very easy fix. We
5 do want you to have that clarity where you know if
6 it's us, the NYPD, using the drone versus a media
7 company using the drone. So that's something that we
8 could definitely build a mechanism for to make sure,
9 you know, the members of the council are aware if
10 we're going to use drone technology in the district.

11 CHAIRPERSON HANKS: Thank you so much. I
12 did want to have-- I had some questions on like
13 social media analysis tools and like Shot Spotter.
14 According to the NYPD's report, the Shot Spotter
15 system records one second before and one second after
16 a gun shot. However, there are several reports from
17 advocates that demonstrate that the system's
18 recordings often beyond this second-- this one-second
19 window. Can you confirm that the audio recording
20 received by NYPD is only limited to one second before
21 or after a gunshot, and can you determine the
22 difference between that and Fourth of July fireworks?
23 [inaudible] my neighborhood.

24 DEPUTY COMMISSIONER GERBER: So, to
25 answer your question, when there's a Shot Spotter

2 hit, so to speak, a Shot Spotter is triggered, the
3 audio clip that the NYPD gets has one second before
4 one second after. We're not given some larger audio
5 universe, period. The Shot Spotter system, there is
6 recording that the Shot Spotter System has that goes
7 on for some number of hours, but we don't have access
8 to that. We don't have access to it in real time.
9 We don't have access to it historically.

10 CHAIRPERSON HANKS: Who does have access
11 to it?

12 DEPUTY COMMISSIONER GERBER: Shot Spotter
13 has it. I also do want to just emphasize when I say,
14 you know, there's-- the microphones are on, but
15 they're 30 feet above ground. They're not designed
16 to pick up human conversation and all that, but to
17 the extent there's any confusion about this, I think
18 the confusion about this, I think the confusion is
19 between what is being recorded by Shot Spotter and
20 what the NYPD ever has access to. And what we're
21 talking about is gun shot, one second before, one
22 second after.

23 CHAIRPERSON HANKS: Thank you so much.
24 That concludes my questioning for NYPD. My Chair
25 Gutiérrez?

2 CHAIRPERSON GUTIÉRREZ: Thanks, Chair.

3 Can I-- I just want to finish up the conversation
4 around Digidog. I know that the Mayor has stated
5 multiple times that the roll-out of this device is
6 kind of the beginning, right? There's more. Can you
7 all share if there are any other technologies similar
8 or with the ability to kind of operate in the same
9 way as Digidog? Anything that PD has in the
10 pipeline?

11 CHIEF MADDREY: Not that I'm aware of. I
12 mean, we have an IT Department. They have numerous
13 people that work there that are looking at different
14 technology, but nothing that's been introduced to me
15 yet for a potential roll-out.

16 CHAIRPERSON GUTIÉRREZ: and I know--
17 Chief, thank you. I know you mentioned that you
18 could speak to a handful of incidences where Digidog
19 rolled out. I'm sure you know in the previous
20 Administration when something similar was rolled out,
21 there was a lot of opposition, particularly in
22 communities in central Brooklyn, East New York, that
23 really felt like they would be targeted? How do you
24 feel that you are rolling this device out

2 differently, and how have you integrated that
3 feedback into your decision-making?

4 CHIEF MADDREY: believe it or not, I have
5 requests from community groups, young people. I have
6 actually one sitting on my desk right now in the
7 Bronx. They have a robotics program. They asked if
8 we could bring the Digidog up there. We're going to
9 bring it up there to show it to a group of kids in
10 the Bronx at the Renaissance. Yeah, well--

11 CHAIRPERSON GUTIÉRREZ: She's going to
12 take that up with you.

13 CHIEF MADDREY: I'm going to make sure
14 she's there. But again, you know, I have an ask, and
15 we're going to bring it up there. This is what we
16 need to do. we need to bring Digidog out, and we do
17 bring Digidog out and we let people see exactly how
18 it operates, and I think once people see it, it kind
19 of-- you know, it kind of brings them down and they
20 understand exactly what it is. There's no weapons
21 attached to it. It's-- you know, a robotic way. It
22 can move and operate like a dog. It can do certain
23 things that other robotics we have can't do.

24 CHAIRPERSON GUTIÉRREZ: Yeah.

2 CHIEF MADDREY: and again, it's a tool to
3 save lives. It's a tool to save people more than
4 anything else.

5 CHAIRPERSON GUTIÉRREZ: Understood. And
6 that example of the school is more like a show and
7 tell and kind of like exposure, correct?

8 CHIEF MADDREY: Yes.

9 CHAIRPERSON GUTIÉRREZ: But in instances
10 where communities, for example, like in East New York
11 I remember they were in opposition to the previous
12 Administration's roll-out. What can you say about
13 how you all-- how you will prioritize or the
14 decision-making process behind like where Digidog
15 goes? Is there anything that you can share
16 specifically for advocates that are concerned about
17 like racial profiling?

18 CHIEF MADDREY: Digidog-- again when
19 Digidog is deployed it's usually, you know, under my
20 orders, one of our designees. We're using Digidog
21 for very volatile situations, situations where people
22 are armed, situations where people may need to be
23 rescued. It's not just being used randomly in
24 neighborhoods to walk around. You will not see
25 Digidog doing that. Or if you see it walking around

2 the neighborhood, it's going to be for demonstrate--
3 you know, a demonstrative purpose. I'll probably be
4 there talking to people in the community, let
5 everyone know this is what it's about, but you won't
6 see that. It's used for purposes where there's
7 danger. If someone's safety is in jeopardy, that's
8 what we using Digidog for.

9 CHAIRPERSON GUTIÉRREZ: Thank you.

10 That'll wrap up my Digidog questions. Let me move on
11 to--

12 CHIEF MADDREY: [interposing] I should
13 have brought him here.

14 CHAIRPERSON GUTIÉRREZ: I want to say no,
15 but I'm tempted to be like yes, you should have.
16 What is-- so I want to just switch gears outside of
17 the Post Act? Really curious about policing software
18 and predictive policing software. Do you know, does
19 NYPD use any predictive policing software?

20 DEPUTY COMMISSIONER GERBER: No. The PD
21 does not have a mechanism for predicating future
22 crime.

23 CHAIRPERSON GUTIÉRREZ: So no databases?

24 DEPUTY COMMISSIONER GERBER: We certainly
25 analyze historical data. Humans analyze data. We

2 sometimes use technology to analyze historical data,
3 but in terms of like predicting the future,
4 predicting future crime, we don't have that
5 capability, no.

6 CHAIRPERSON GUTIÉRREZ: Well, some would
7 argue that a database in many ways provides-- does do
8 that.

9 DEPUTY COMMISSIONER GERBER: Well, no,
10 just for example, if we have a crime that's been
11 committed and we're trying to figure out if that
12 links up with some other past crimes-- so a crime has
13 been committed in the past. Is that part of some
14 pattern? Where of course, of course we're going to
15 look at historical data to see if it's a pattern. It
16 would be irresponsible not to. We're going to look--
17 [inaudible] database, we're talking about historical,
18 you know, crime reports, for example. You know,
19 historical data regarding locations of crime or the
20 ammo that was used in a particular crime, in those
21 situations we're going to look at that historical
22 data to try to solve crimes that have been committed,
23 but that is very different, categorically different
24 than some sort of predictive policing.

2 CHAIRPERSON GUTIÉRREZ: Thank you. I know
3 that the members had asked about facial recognition.
4 Is there anything that you can speak to regarding
5 voice recognition? I read a number of examples where
6 potentially of like cellphone equipment can be
7 utilized to capture information from folks. I think
8 it might even be on one of the devices that you're
9 utilizing, but is voice recognition a feature of any
10 of the surveillance tools that you use?

11 DEPUTY COMMISSIONER GERBER: I'm not sure
12 exactly what you're referring to, but I believe the
13 answer is no. We don't-- I'm not 100 percent sure I
14 know what you're referring to, but again, if I
15 understand you correctly, the answer is no.

16 CHAIRPERSON GUTIÉRREZ: But, so I think
17 plainly, are there any devices or surveillance tools
18 that the PD has that are for like the intent of
19 capturing voices or conversations--

20 DEPUTY COMMISSIONER GERBER: [interposing]
21 Oh, well, sure. I mean, we-- sorry. We, of course,
22 in undercover operations we'll sometimes record
23 conversations, right? So undercover recording
24 devices which have come up a number of time. We
25 also, as you know, we have court-authorized wire

2 taps, for example, and there's a rigorous legal
3 process for that. It requires a court authorization,
4 frankly authorization and a showing that goes beyond
5 probable cause for court-authorized wire taps. So
6 there are scenarios where we are recording what
7 people say consistent with the law. I mean,
8 obviously, there are very strict rules about when
9 we're allowed to do that and how we can do that, and
10 the necessary court authorizations for doing that.
11 But I thought you were asking about sort of voice
12 recognition. I think that's a little different, and
13 that's what I was a little confused about.

14 CHAIRPERSON GUTIÉRREZ: But I think you
15 answered it. I think it sounds like no. I want to
16 just kind of jump back-- jump a little bit related
17 to--

18 DEPUTY COMMISSIONER GERBER: [interposing]
19 Actually, Chair, if I may just for one moment, just I
20 want to clarify one thing. There is-- because the
21 voice recognition issue where it does come up, we are
22 not using yet. There have been public reports about
23 Truelio [sic], and that-- so there's been public
24 reporting about this. We're considering what if
25 anything to do with Truelio. There is a contract.

2 If we decide to go ahead with a Truelio pilot and
3 using Truelio, that is a-- it easily uses AI. It's
4 vice analytics. It's voice analytics. Part of voice
5 analytics-- I'm not an expert on this, but as we're
6 talking about-- voice analytics is going to include
7 obviously the ability to recognize and distinguish
8 between voices. But I just want to be very, very
9 clear. We are not doing that now. And if we were to
10 start using voice analytics, which maybe is what
11 you're questions is getting at, we would have to do a
12 new IUP. That would be a new surveillance technology
13 for us, voice analytics, and we would have to do a
14 whole new IUP which would describe what we're
15 planning to do, and there would be a comment period
16 for that.

17 CHAIRPERSON GUTIÉRREZ: Okay. Go ahead.

18 CHAIRPERSON HANKS: Thank you so much,
19 Chair Gutiérrez. I have one question just off of
20 that. Is NYPD currently using any AI to review
21 footage received from surveillance technology, body
22 cams, drones?

23 DEPUTY COMMISSIONER GERBER: No, no.

24 CHAIRPERSON HANKS: Thank you.
25

2 CHAIRPERSON GUTIÉRREZ: Thank you, Chair.

3 My next question is related to the OIG report,
4 specifically this might be also for OTI, related to
5 social media. According to the report, PD creates
6 fake social media accounts to obtain information
7 during investigations. What are the guidelines on
8 how these accounts are used, and how are they
9 enforced?

10 DEPUTY COMMISSIONER GERBER: So, there
11 are guidelines. We have-- there's certainly internal
12 policies about undercover accounts. I don't have
13 that at the ready here. What I will say and I think
14 it's important to emphasize, is that in the same way
15 that we do undercover operation's traditionally, you
16 know, out in the field so-to-speak, which involves
17 officers in an undercover capacity, we also will have
18 officers in an undercover capacity at times on social
19 media out in the virtual world, so to speak.

20 CHAIRPERSON GUTIÉRREZ: But those
21 guidelines are not made public, or they're not
22 accessible?

23 DEPUTY COMMISSIONER GERBER: No, I-- my
24 understanding is those guidelines are not public.

2 CHAIRPERSON GUTIÉRREZ: Can they be made
3 public?

4 DEPUTY COMMISSIONER GERBER: I'm
5 certainly not going to commit to that sitting here
6 right now, and I have to emphasize, you know, you can
7 imagine why there would be operational concerns, very
8 significant operational concerns about providing
9 public information about under-- how we use
10 undercover accounts. So, I, sitting here today
11 cannot commit to that, absolutely not.

12 CHAIRPERSON GUTIÉRREZ: Thank you. in
13 the same-- in a similar OIG report, social network
14 analysis tools use AI to search and monitor social
15 media, and pursuant to Local Law 35, the OTI shall
16 publish all automated decision-making systems used by
17 agencies including artificial intelligence systems.
18 However, social network analysis tools were not
19 listed in OTI's report. What is the reason?

20 DEPUTY COMMISSIONER GERBER: I'll take
21 that. Our social media analysis tools do not use AI.
22 We're not using AI on social media. We do searches
23 and we look at relationships between individuals as
24 part of investigations, but to the extent the
25 question is are we applying AI at our sort of social

2 media searches, my understanding is that the answer
3 to that is no.

4 CHAIRPERSON GUTIÉRREZ: Okay. Okay.
5 We're doing so good on time, y'all. I want to just
6 ask about some more contract questions. Is every
7 contract with PD related to surveillance technology a
8 part of city records?

9 CHIEF CONTRACTING OFFICER MENDOZA: When
10 you say a part of city records, like you mean that
11 it--

12 CHAIRPERSON GUTIÉRREZ: [interposing] Is
13 it public?

14 CHIEF CONTRACTING OFFICER MENDOZA: So,
15 any new contract that we procure is going to have to
16 go into City Administrative Systems. Procurements
17 generally require public notice. Anything over 100K
18 is going to have to have a public notice both for
19 solicitation and for award, so those things would be
20 publicly available.

21 CHAIRPERSON GUTIÉRREZ: And is every
22 such-- can every such contract be found on Checkbook?

23 CHIEF CONTRACTING OFFICER MENDOZA: They
24 should, yeah. Every procurement we do when it's
25 registered will show up in Checkbook.

2 CHAIRPERSON GUTIÉRREZ: Are there any
3 agreements between NYPD and other agencies to keep
4 the existence of contracts confidential?

5 CHIEF CONTRACTING OFFICER MENDOZA: Not
6 to my knowledge.

7 CHAIRPERSON GUTIÉRREZ: Do you know if
8 you have any existing FOIL requests related to
9 contracts or?

10 CHIEF CONTRACTING OFFICER MENDOZA: We
11 certainly get a number of FOIL requests. I don't have
12 any information about anything active.

13 CHAIRPERSON GUTIÉRREZ: I'm well aware
14 you get a lot of FOIL requests. What is the-- and I
15 know there are plenty of advocates who will testify
16 on this today, but what is the process for getting a
17 response for said FOIL request? How many people in
18 the agency are working on FOIL requests?

19 DEPUTY COMMISSIONER GERBER: I'll take
20 that. We have a whole FOIL team. I don't have the
21 exact numbers here in front of me in terms of how
22 large the team. We certainly can get that. We
23 certainly can get you that information.

24

25

2 CHAIRPERSON GUTIÉRREZ: But you don't
3 know? You don't know how long it takes for a
4 response to a FOIL requests?

5 DEPUTY COMMISSIONER GERBER: Oh, sorry,
6 it thought you meant the number of people involved.
7 The time it can take can vary tremendously depending
8 on the nature of the request. There are FOIL
9 requests that are very straightforward. There are
10 FOIL requests that are incredibly complex. Some that
11 can be done in a short period of time, some that
12 require frankly a very significant undertaking in
13 terms of time and resources. It's going to vary
14 tremendously depending on the nature of the request.

15 CHAIRPERSON GUTIÉRREZ: Do you know if
16 you have outstanding FOIL requests older than a year
17 old?

18 DEPUTY COMMISSIONER GERBER: So, we
19 certainly have a backlog. We have undertaken
20 actually recently to try to really work through that
21 backlog, put additional resources into FOIL, getting
22 additional individuals to work on that backlog. I
23 don't have the data here with me, but we are working
24 to cut into that backlog.

2 CHAIRPERSON GUTIÉRREZ: But do you
3 believe that there are probably requests older than a
4 year old?

5 DEPUTY COMMISSIONER GERBER: It certainly
6 is possible, yes.

7 CHAIRPERSON GUTIÉRREZ: Older than two?

8 DEPUTY COMMISSIONER GERBER: I don't
9 know.

10 CHAIRPERSON GUTIÉRREZ: Do you see where
11 I'm going with this?

12 DEPUTY COMMISSIONER GERBER: There is a
13 backlog and we are working on it.

14 CHAIRPERSON GUTIÉRREZ: Yeah.

15 DEPUTY COMMISSIONER GERBER: And to your
16 point, we need to cut into that backlog. There is a
17 resource issue here in terms of--

18 CHAIRPERSON GUTIÉRREZ: [interposing]
19 Sure.

20 DEPUTY COMMISSIONER GERBER: We have
21 gotten additional individuals assigned to work just
22 on working on this backlog. That's a project that
23 we've undertaken, and it is ongoing.

24 CHAIRPERSON GUTIÉRREZ: And you don't
25 have a sense of if that means hiring more people?

2 DEPUTY COMMISSIONER GERBER: No, no, so
3 we've gotten some officers temporarily assigned to
4 us. They're not permanently part of the legal
5 bureau, but they've come to us for some period of
6 time just to work on this backlog. That was we cited
7 personal. We have problem here. We have this
8 backlog. We need to really cut into it, reduce that
9 back log, and the way to do that is by getting
10 additional personnel to work on that, at least on a
11 temporary basis, and that's what we've done.

12 CHAIRPERSON GUTIÉRREZ: Do you have a
13 sense if these are existing personnel members that'll
14 be switching gears to this project or are brand new
15 hires?

16 DEPUTY COMMISSIONER GERBER: No, no,
17 they're not new hires. These are restricted
18 personnel. These are officers who for one reason or
19 another can't right now be out in the field, and a
20 very good way to deploy their abilities if they can't
21 be out in the field is to have them working to get
22 through this FOIL backlog.

23 CHAIRPERSON GUTIÉRREZ: Thank you. My
24 next question is related to-- in the instance where
25 PD is deploying new surveillance technology, is there

2 communication with OTI at some point during that
3 process?

4 CHIEF PRIVACY OFFICER FITZPATRICK: So,
5 my conversations, again, when we look to the Office
6 of Technology and Innovation very intentionally so,
7 we've got subject-- the citywide subject matter
8 expertise across various verticals. So for example,
9 my area is information privacy. My common touch-
10 point at the agency level is the Agency Privacy
11 Officer, and with NYPD during my tenure I had had
12 conversations about surveillance technology
13 periodically.

14 CHAIRPERSON GUTIÉRREZ: Sure, and is OTI
15 in those scenarios giving an approval or consulting?
16 Kind of-- what is that? What are those
17 conversations?

18 CHIEF PRIVACY OFFICER FITZPATRICK: As I
19 mentioned earlier, Chair, the agency at large
20 generally does not handle procurements for individual
21 agencies. We negotiate-- the agency negotiates
22 citywide contracts. Agency-- from my area of
23 responsibility, agencies are very intentionally
24 empowered to utilize technology, and in the context
25 of information privacy through the lens of the

2 identifying information law with the individual
3 analysis through their particular mission or purpose,
4 recognizing each agency is the expert of its own
5 field, my office is available to provide feedback,
6 guidance, perspective as necessary to any agency
7 privacy officer.

8 CHAIRPERSON GUTIÉRREZ: and in those
9 scenarios where you are providing feedback, if PD is
10 requesting funding for said technology, does that go
11 to OTI for some level of approval?

12 CHIEF PRIVACY OFFICER FITZPATRICK: For
13 funding my understanding is no, but again, that's not
14 my area.

15 CHAIRPERSON GUTIÉRREZ: Funding the
16 specific technology, equipment or program.

17 CHIEF PRIVACY OFFICER FITZPATRICK:
18 Correct. So my understanding of that is no. Again,
19 the agency generally does not handle individual
20 procurement for agencies, and I'm unaware of any
21 procurements for the Police Department as it relates
22 to surveillance technology.

23 CHAIRPERSON GUTIÉRREZ: That sounds right
24 to you all? That checks out as well?

2 DEPUTY COMMISSIONER GERBER: Yes,
3 absolutely.

4 CHAIRPERSON GUTIÉRREZ: Okay, thank you.
5 And-- okay, well then that changes my next few
6 questions. Okay, I guess my last question is related
7 to social media monitoring. What tools does the PD
8 use for social media monitoring? How much can you
9 share?

10 DEPUTY COMMISSIONER GERBER: So, we
11 certainly in the course of criminal investigations
12 will run searches across publicly-available social
13 media. It's very important to emphasize, publicly
14 available. And in the course of a criminal
15 investigation, in the same way that we try to get
16 information, you know, out on the street, so to
17 speak, we can all try to do that on social media by
18 running searches across publicly available
19 information. And then in particular, in the same way
20 you would in a sort of traditional investigation,
21 identifying connection between people that are
22 publicly available. So we certainly do that in the
23 course of criminal investigations.

24 CHAIRPERSON GUTIÉRREZ: And does OTI
25 provide any guidance for utilizing these websites,

2 these publicly available platforms, or you can--
3 you're utilizing these tools independently, not-- you
4 don't-- you're not checking in with OTI?

5 CHIEF PRIVACY OFFICER FITZPATRICK: So,
6 thank you for that clarifying question, Chair, and I
7 think it's a really important one. As I mentioned,
8 when we look at that individual analysis on the
9 agency level about evaluating collections or
10 disclosures of identifying information, empowering
11 the role of the agency privacy officer. We also as a
12 matter of citywide privacy policy enumerate a number
13 of privacy principles to help support agency
14 decision-making as it relates to identifying
15 information citywide with the guidance that agencies
16 consider them in all decision-making as it relates to
17 identifying, but recognizing that each individual
18 agency is going to have a unique analysis as it
19 relates to own mission and purpose.

20 CHAIRPERSON GUTIÉRREZ: And that's a
21 good-- that's great. That's a sufficient answer. Is
22 there-- just separate from this conversation with PD,
23 does OTI provide guidance on this kind of technology,
24 particularly with accounting for bias, like for
25 example.

2 CHIEF PRIVACY OFFICER FITZPATRICK: So,
3 thank you for that question as well, Chair. I think
4 it highlights an important point. Certainly, when
5 you're discussing bias you're likely going to
6 encounter that decision in the world of leveraging
7 artificial intelligence, for example. And as I think
8 the Council is aware, OTI and the City announced its
9 artificial intelligence action plan just about a
10 couple months ago now I think, which I think is quite
11 a robust undertaking in terms of very specific action
12 items to develop a governance structure on a citywide
13 level as it relates to the utilization of this new
14 technology. that work-- and I think also quite boldy
15 calls for the majority of the called upon action
16 items to either be completed or initiated within one
17 year form publication, including multiple touch-
18 points with stakeholders throughout that process, by
19 virtue of setting up advisory committee's public
20 engagement, and inclusive consideration of the very
21 important issue of bias.

22 CHAIRPERSON GUTIÉRREZ: Thank you. What
23 mechanisms are in place to protect the privacy of
24 individuals who may be inadvertently captured by NYPD
25 surveillance technologies?

2 DEPUTY COMMISSIONER GERBER: I think it's
3 going to depend on the nature of the surveillance
4 technology. I think it's something we are very
5 sensitive to, of course, but it's hard to answer that
6 at a global way.

7 CHAIRPERSON GUTIÉRREZ: Yeah.

8 DEPUTY COMMISSIONER GERBER: Really,
9 obviously that tissue comes up in various
10 surveillance technologies. You know, in some context
11 when you're getting a warrant for something, for
12 example, they're going to-- the warrant itself and
13 the court order may put in place a variety of
14 restrictions of limitation on what we even can do
15 because of those concerns. In the court-authorized
16 wire-tapping context, for example, there are very
17 strict rules about minimization on court-authorized
18 wire taps because of the issues that you're
19 identifying in terms of, you know, innocent third
20 parties. But the answer to that really does depend
21 on the nature of the particular surveillance
22 technology, and the, you know, particular issues that
23 might arise.

24 CHAIRPERSON GUTIÉRREZ: Is there a
25 process for retaining or deleting any of that data

2 that-- for those innocent individuals that's
3 collected through surveillance technology?

4 DEPUTY COMMISSIONER GERBER: Right, so
5 it's going to just depend on the particular
6 surveillance technology. to go back to the court-
7 authorized wire taps, just as an example, in the
8 nature of a court-authorized wiretap, you're almost
9 certainly going to end up sometimes with
10 interceptions of individuals who are, you know,
11 innocent civilians and there are very strict rules
12 imposed by statute as to minimization, to make sure
13 that you're not listening to more of those
14 conversations. You know, to the extend you're
15 intercepting those conversations, they're walled off.
16 So, you know, there are going to be rules and
17 procedures in place, but it will vary by the nature
18 of the surveillance technology.

19 CHAIRPERSON GUTIÉRREZ: In those
20 instances are people made aware that they're being--
21 that their like face or voice are being captured in
22 surveillance technology?

23 DEPUTY COMMISSIONER GERBER: so, again,
24 as using the court-authorized wiretap example, the
25 statute actually provides the basically-- at the

2 conclusion of a court-authorized wiretap, individuals
3 who are intercepted on the wiretap need to be
4 notified.

5 CHAIRPERSON GUTIÉRREZ: Okay.

6 DEPUTY COMMISSIONER GERBER: So, that's
7 an example where, you know, exactly, those
8 individuals are told there's a whole sort of
9 statutory regime for that.

10 CHAIRPERSON GUTIÉRREZ: and does OTI play
11 a role in overseeing that, that they have to be told
12 or any of that? Or what-- does OTI play any kind of
13 role in that?

14 CHIEF PRIVACY OFFICER FITZPATRICK: For
15 advising in the context of criminal investigations,
16 no.

17 CHAIRPERSON GUTIÉRREZ: For-- no, no. In
18 the example of having to notify people, innocent
19 folks, that they're being captured to some capacity
20 in surveillance equipment or technology?

21 CHIEF PRIVACY OFFICER FITZPATRICK: so,
22 my understanding is no. The circumstances in which
23 individual notification manifests in the context of
24 my area of responsibility is when there has been an
25 unauthorized disclosure of identifying information by

2 a city agency. We provide guidance to agency privacy
3 officers when and under which circumstances ought to
4 be and should be notified of those occurrences
5 depending on the data elements at issue.

6 CHAIRPERSON GUTIÉRREZ: Thank you. I
7 think-- are we waiting for [inaudible]? OH, she's
8 coming back. Okay, sorry. I'm trying to just milk
9 every minute that you guys are here. Can I just jump
10 to the DAS system, the Domain Awareness System, just
11 a couple question? Yeah? How do NYPD personnel
12 receive authorization to access that system, and do
13 they receive training on the use of it?

14 CHIEF MADDREY: All of our members have
15 access to the DAS--

16 CHAIRPERSON GUTIÉRREZ: [interposing] Is
17 your mic on? I'm sorry.

18 CHIEF MADDREY: I did turn it off, I'm
19 sorry, forgive me. All of our members have access to
20 the DAS, Awareness System. They may not know how to
21 work every individual search engine, but a lot of the
22 basic work are complaint reports or accident reports,
23 [inaudible] reports all link to the DAS system. All
24 our officer have access to the DAS.

2 CHAIRPERSON GUTIÉRREZ: And do they
3 receive training on it?

4 CHIEF MADDREY: They receive training on
5 how to do complaint reports, how to do accident
6 reports, and then when we develop new search engines
7 or new protocols, depending on what it is, officers
8 will get trained on it.

9 DEPUTY COMMISSIONER GERBER: I do want to
10 emphasize that the Domain Awareness System, DAS, it's
11 bringing together information from other sources,
12 right? Just so there's no confusion. It's not like
13 DAS itself, the Domain Awareness System, is somehow
14 conducting surveillance. It's other surveillance
15 technologies feed into the DAS system-- to DAS so
16 that a police officer who's trying to investigate
17 something, it's one place they can go to and bring
18 together multiple sources of information.

19 CHAIRPERSON GUTIÉRREZ: And do you-- is
20 there a way that the agency audits personnel use of
21 this system? Is there any-- are there scenarios
22 where members are using DAS for personal purposes?
23 I'm trying to get to the issue of misuse of the
24 system.

2 CHIEF MADDREY: There's a footprint.

3 When you use DAS, you leave a footprint. So if I
4 sign into something right now it says, Jeff Maddrey--

5 CHAIRPERSON GUTIÉRREZ: [interposing] It
6 logs in.

7 CHIEF MADDREY: signed in, right. So, if
8 we become aware of some misuse or some misconduct, an
9 internal investigation-- our Internal Affairs do have
10 the ability to go back and see who looked at what or
11 who used what.

12 CHAIRPERSON GUTIÉRREZ: and how does the
13 PD address that? How do you address that?

14 CHIEF MADDREY: We have strict policies
15 about computer misuse, using computers for personal
16 or business. We have strict policies for that.
17 Officers who are found to violate that policy, it's
18 strict punishment.

19 CHAIRPERSON GUTIÉRREZ: Okay. And while
20 the 2021 Impact and Use Policy states that the DAS
21 itself does not use video analytics, biometric
22 measurements technologies, or facial recognition
23 technologies, can data produced by the DAS be
24 utilized by other tools that do use those
25 technologies? Are there screen grabs? Are there

2 still images? Are there any way that information on
3 the DAs can be used for any of those technologies?

4 DEPUTY COMMISSIONER GERBER: I'm not sure
5 I totally understand the question. I think it's
6 almost the other way around. In other words, we have
7 information we gain from other surveillance
8 technologies that feeds into DAS, and DAS is sort of
9 a repository and a means of bringing together those
10 different sources of information. I'm not sure that
11 answers your question.

12 CHAIRPERSON GUTIÉRREZ: I guess I was
13 asking if the reverse is possible?

14 DEPUTY COMMISSIONER GERBER: Right, but
15 DAS itself is not a mechanism for surveilling
16 anybody. It's taking it from other sources and
17 bringing it together.

18 CHAIRPERSON GUTIÉRREZ: And so DAS does
19 not have any capability to share video images?

20 DEPUTY COMMISSIONER GERBER: Well, no,
21 just to be clear, if you're watching a video or you
22 see a photo whether it's on DAS or otherwise, someone
23 capable of, you know, screen grab or capturing that
24 in some way, yes, and if that's being done, you know,
25 in an inappropriate way, it being misused in some

2 way, as the Chief said, that person is subject to
3 disciplinary action.

4 CHAIRPERSON GUTIÉRREZ: And do you--
5 similarly, Chief, to how you're able to see who
6 logged in and how they're accessing it, are you able
7 to tell when information on the system is being
8 screen grabbed?

9 DEPUTY COMMISSIONER GERBER: I don't
10 know.

11 CHAIRPERSON GUTIÉRREZ: The technology
12 exists. I just want to let you know, Snapchat
13 figured that out a long time ago.

14 CHIEF MADDREY: we may not be aware if--
15 and I don't know if I can answer that for certain.
16 We may not be aware if they grab just the image, but
17 we will be aware that they pulled the image up. So
18 we'll know that hey, if there's an image that's
19 compromised, we will know who pulled that image up.

20 CHAIRPERSON GUTIÉRREZ: Okay. Thank you.
21 I have a-- I'm just going to ask [inaudible]
22 question, and then I'm done. So I just want to-- I
23 know that Council Member Cabán asked the question.
24 We didn't get to hear the answer. So I'll just--

1 COMMITTEE ON PUBLIC SAFETY WITH COMMITTEE ON TECHNOLOGY 124

2 DEPUTY COMMISSIONER GERBER: [interposing]

3 Yeah.

4 CHAIRPERSON GUTIÉRREZ: Do you remember
5 the question?

6 DEPUTY COMMISSIONER GERBER: I do. I do.

7 CHAIRPERSON GUTIÉRREZ: Okay, okay.
8 [inaudible] have that on the record.

9 DEPUTY COMMISSIONER GERBER: Yes,
10 absolutely. I said that I did not accept the premise
11 of her question, but I also wanted to add that we
12 follow the law, we follow state law, city law. To
13 the extent she was suggesting that are we taking
14 steps to evade requirements under the law, the answer
15 is no.

16 CHAIRPERSON GUTIÉRREZ: Thank you.
17 Chair?

18 CHAIRPERSON HANKS: Thank you so much.
19 My questions-- do I have any other Council Members
20 who have questions before the release the NYPD at
21 3:30 on the dot? Good stuff. Thank you so much for
22 your testimony and your answering the questions, and
23 now we will have DOI coming up.

24 CHAIRPERSON GUTIÉRREZ: Thank you.
25 Looking forward to the follow-up.

2 CHAIRPERSON HANKS: Thank you.

3 Would you like me to start? Okay. You
4 have not sworn me in. I'm just letting you know
5 that--

6 COUNCIL MEMBER BREWER: [interposing] I
7 told them you were honest.

8 COMMISSIONER STRAUBER: In case you would
9 like to. Thank you, Chair Brewer. I appreciate the
10 confidence. Good afternoon. My name is Jocelyn
11 Strauber. I'm the Commissioner of the Department of
12 Investigation. Thank you, Chair Gutiérrez, members
13 of the Committee on Technology and Chair Hanks,
14 members of the Committee on Public Safety for the
15 opportunity to speak about DOI's oversight role with
16 respect to the NYPD's use of surveillance technology
17 as set out in the public oversight of surveillance
18 technology legislation which I'll refer to as the
19 POST Act. As you know, DOI oversees the operations,
20 policies, programs and practices of the New York City
21 Police Department through our Office of the Inspector
22 General for the NYPD. The POST Act requires NYPD to
23 produce and publish Impact and Use Policies, IUPs for
24 short, for each surveillance technology used by the
25 NYPD and directs OIG-NYPD to prepare an annual audit

2 of the Department's compliance with these IUPs.

3 Today, I will give you a summary of DOI's findings

4 from our first annual report pertaining to the POST

5 Act, speak briefly about the focus of our second

6 report which is currently in draft, and also share

7 our view of the three proposed bills under

8 consideration today with respect to the NYPD's use of

9 surveillance technology. Before I begin, I want to

10 recognize Inspector General Jeanene Barrett, who I

11 appointed to that permanent position in August. She

12 unfortunately could not be here today as planned, but

13 I am very proud to be working with her. She has led

14 the OIG-NYPD since January 2022, initially as the

15 Acting Inspector General and brings critical

16 experience to this role in relevant areas including

17 police oversight and accountability, community

18 engagement, and supporting underserved communities.

19 Now, let me turn to our November 2022 report, our

20 assessment of the NYPD's response to the POST Act. In

21 November 2022, we issued our first report pursuant to

22 the POST Act. The report was the result of an in-

23 depth examination in which OIG-NYPD interviewed a

24 range of individuals including NYPD officials,

25 members of the advocacy community who called for the

2 legislation that ultimately became the POST Act, and
3 experts on various surveillance technologies. For
4 this first report, the OIG-NYPD reviewed all
5 published IUPs and performed a section-by-section
6 assessment of one IUP, and an in-depth assessment of
7 two selected surveillance technologies, and compared
8 the POST Act to similar statutes in other
9 jurisdictions to better understand other models for
10 achieving transparency and public engagement in this
11 area. While the OIG-NYPD investigative team found
12 that NYPD largely complied with the technical POST
13 ACT requirements, it also found that the IUPs did not
14 contain sufficient detail to allow for a full
15 assessment of NYPD's compliance with those IUPs, as
16 the statute requires. OIG-NYPD concluded that
17 improvements to the IUPs would enable more robust
18 oversight, as well as more transparency with respect
19 to the nature and use of these technologies.
20 Specifically, the IUPs contained certain overly
21 general language that failed to provide sufficiently
22 specific information about the nature of the
23 technologies, the retention period for data obtained
24 via use of the technologies, and the entities with
25 which the data can be shared. Per our assessment,

2 the broad and non-specific language within the IUPs
3 failed to provide clear direction to NYPD and
4 sufficiently concrete information to the public in
5 these and other areas. Additionally, OIG-NYPD
6 interprets the POST Act to require an IUP for each
7 unique surveillance technology and disagrees with
8 NYPD's view that grouping of technologies is
9 permitted as a general matter. While grouping may be
10 appropriate for devices that use identical or very
11 similar technologies, OIG-NYPD is concerned that
12 grouping of related surveillance technologies into
13 single IUPs is inconsistent with the spirit, if not
14 the letter of the POST Act. Grouping may mask
15 certain unique technological capabilities because
16 they may not be publicly disclosed at all, as they
17 will be deemed "covered" by an existing IUP.
18 Furthermore, because there will be no new IUP
19 applicable to those new technological capabilities,
20 there will be no opportunity for public comment on
21 those policies. It is also difficult for OIG-NYPD to
22 meaningfully assess NYPD's compliance with the IUP
23 when the IUP applies to various technologies that
24 could have different functions or capabilities.
25 Based on its review, OIG-NYPD issued 15 policy and

2 procedure recommendations to NYPD in November of
3 2022. I want to be clear that many of these
4 recommendations went beyond the requirements that the
5 POST Act imposes, and that we made these
6 recommendations to enhance public transparency with
7 respect to NYPD's use of surveillance technology.
8 Equally important, the recommendations are intended
9 to be sensitive to the need to protect confidential
10 law enforcement information. For the most part, as
11 the report made clear, and with the exception of
12 NYPD's practice with respect to grouping, we did not
13 find that NYPD had violated the POST Act. The
14 recommendations advised the NYPD to issue an IUP for
15 each individual surveillance technology, to ensure
16 that each IUP contains specific information such as
17 the names of the entities with which the NYPD can
18 share surveillance data as well as specific
19 safeguards or restrictions on the use or
20 dissemination of the surveillance data, and to
21 describe the potential disparate impacts on protected
22 groups of the use and deployment of the surveillance
23 technology. OIG-NYPD also requested an itemized list
24 of all surveillance technologies used by NYPD, in
25 order to determine whether grouping of multiple

2 devices or technologies under a single IUP was
3 appropriate. NYPD previously rejected OIG-NYPD's
4 recommendation to provide an itemized list of the
5 surveillance technologies that it uses, but the NYPD
6 has since agreed to provide this itemized list. We
7 look forward to receiving that list so that we can
8 further consider the question whether any
9 technologies currently grouped within a single IUP in
10 fact require distinct IUPs. The OIG-NYPD recommended
11 that NYPD convene a working group that included NYPD
12 personnel, relevant City Council members, and
13 representatives from select advocacy groups with
14 expertise in surveillance technologies to make
15 recommendations to NYPD on any necessary updates to
16 existing IUPs, for example recommending updates to
17 IUPs to reflect disparate impact of technologies.
18 Other recommendations included strengthening internal
19 tracking of each instance when NYPD provides an
20 external agency with data collected via its
21 surveillance technologies and other transparency
22 measures. With the exception of our recommendation
23 that DOI receive an itemized list of technologies,
24 NYPD has rejected all of our POST Act report
25 recommendations. Let me just speak for a moment to

2 our ongoing roles in the auditing process. We
3 understand the relevant and important concerns about
4 the use of surveillance technology in New York City
5 and we are committed to providing oversight in this
6 important area. I want to be clear that an annual
7 comprehensive inquiry into the NYPD's compliance with
8 each of its three dozen IUPs, for more than 80
9 surveillance technologies, is not a feasible
10 undertaking for DOI. For that reason, both in last
11 year's annual report and in the one we plan to issue
12 in the first quarter of 2024, which will cover this
13 calendar year, we are focused on particular
14 surveillance technologies of public interest and
15 concern, as well as broader issues with respect to
16 the POST Act's requirements and NYPD's compliance
17 more generally. In our upcoming report to be issued
18 in the first quarter of next year, we will discuss
19 NYPD's compliance with the POST Act with respect to a
20 group of technologies of particular public interest,
21 including Digidog and the Autonomous Robot, which I
22 believe is referred to as K5. We have reviewed
23 Introductions 1193, 1195, and 1207, which are being
24 considered at today's hearing, and we are broadly
25 supportive of the three bills as they generally track

2 several of our recommendations from the 2022 report.
3 We look forward to working with the Council on these
4 bills if they move forward to a vote. Thank you for
5 your time, and I'm happy to take any questions that
6 you have.

7 CHAIRPERSON HANKS: Thank you so much.
8 That was great. I appreciate that. We talk about
9 your testimony in particular, you said that for that
10 reason, both in last year's annual report and we plan
11 to issue the first report of the first quarter of
12 2024. You're focused on particular surveillance
13 technologies of public interest and concerns as well
14 as broader issues with respect to the POST Act
15 requirements of NYPD's compliance more generally.
16 And then you went on to say those particular public
17 interests are Digidog and the autonomous robot. Am I
18 correct in saying that those are the two that you're
19 going to focus on in particular?

20 COMMISSIONER STRAUBER: We are going to
21 focus on those. There are several others that we
22 will be considering as well.

23 CHAIRPERSON HANKS: And why-- out of all
24 of them, why is it a particular interest to look at
25 Digidog and the autonomous robot?

2 COMMISSIONER STRAUBER: Well, I think as
3 today's hearing and your questions show, there is
4 some public concern about how these technologies are
5 going to be used and deployed. There has been an
6 announcement, you know, that referenced here today,
7 but this is sort of the beginning of a wave of more
8 technology of this nature. And while fully
9 recognizing the importance of the use of these
10 technologies for public safety, I think there's a
11 public interest and better understanding how they
12 work and the rules and regulations that apply to them
13 through the Police Department's implementation, and
14 that's why we've chosen to focus on those.

15 CHAIRPERSON HANKS: Thank you. Do you
16 believe that NYPD's grouping of the related
17 technologies into a single IUP can be used to obscure
18 the Department's specific use of technology, and what
19 applicable policies apply to what technology?

20 COMMISSIONER STRAUBER: So, I think it
21 can be. Grouping, I think, can obscure not only the
22 particular-- it can obscure first of all what are the
23 technologies being used, right? Because if there is
24 no impact and use policy which also describes the
25 general purpose of the technology and how it's used,

2 if there are technologies that are grouped and
3 therefore not specifically referred to in the policy
4 applicable to a particular area, let's say, then I
5 think it can obscure the types of technologies that
6 are using-- that are being used by the P-D. I think
7 this is a fact-specific inquiry, however. There may
8 well be types of technologies that are sufficiently
9 similar such that the kind of detail that an IUP
10 calls for is not required for each individual device,
11 for example, as which was the language that was used
12 in the Police Department's testimony. It's entirely
13 possible that describing general types of technology
14 works much of the time. What we want to do and what
15 our recommendation and specifically our request for
16 that itemized list is designed to affect, we would
17 like to know what all of the technologies are, that
18 in theory fall within let's say one or two IUPs, if
19 there are multiple technologies. And we want to be
20 able to then consider ourselves how are these used,
21 and does the IUP fully describe and encompass the
22 capabilities and functionalities, the rules that
23 apply to these technologies.

24 CHAIRPERSON HANKS: I appreciate that.

25 And I'm following you, and so do you think that

2 there's a space in which they don't think that the
3 grouping needs to be done, or the grouping that
4 they're doing is sufficient because they're not
5 looking for what we would be looking for or the
6 public would be looking for?

7 COMMISSIONER STRAUBER: you know, there
8 might be. I think the inquiry that we're doing in
9 the upcoming report will touch on this issue, because
10 we heard today and my understanding is that Digidog,
11 for example, is included in the IUP for situational
12 awareness cameras. And so we will undertake as we
13 look at this issue an inquiry as to whether that is
14 sufficient to describe to the public the capabilities
15 of that technology, and I don't want to get ahead of
16 myself because we don't have a final report yet, but
17 I expect those are the type of questions that we will
18 consider in the report that will come out next year.

19 CHAIRPERSON HANKS: Is there ever a time
20 which NYPD would say, you know, we don't want to do
21 this because of sensitive information and a space
22 where DOI would want that information for a different
23 reason? Does that make sense?

24 COMMISSIONER STRAUBER: Well, I think in
25 terms of the information we receive, we've developed

2 a very productive relationship with the Police
3 Department and I expect we will get all of the
4 information that we're asking for to prepare this
5 report. I could envision situations where there's
6 concern about certain types of disclosure of
7 information or where the Police Department-- and we
8 heard some of this today, doesn't want to go into
9 detail about certain devices, because there might be
10 a risk that that compromises a law enforcement
11 operation or interest. I could see that, and if that
12 comes up we would have a conversation about that.

13 CHAIRPERSON HANKS: And as you said in
14 your testimony, that the bills that have been
15 proposed today would speak to that or would at least
16 give us as legislators and governmental people who
17 have the ability for oversight, you think that those
18 bills would give us what we needed to kind of find
19 that middle ground?

20 COMMISSIONER STRAUBER: Well, I think the
21 bill's track certain of our recommendations with
22 regard to providing more information to the public,
23 and with regard to how the IUPs are designed. I
24 think at another time we could get into more of a
25 discussion about sort of the nitty gritty of the

2 language of the proposed legislation, because we
3 might have some proposals there, but generally I
4 think they track our recommendations and they
5 accomplish some of the things that we sought to
6 accomplish in our report.

7 CHAIRPERSON HANKS: And they meaning the--
8 my colleague--

9 COMMISSIONER STRAUBER: [interposing] the
10 legislation.

11 CHAIRPERSON HANKS: My colleague's, okay,
12 that's great.

13 COMMISSIONER STRAUBER: Correct.

14 CHAIRPERSON HANKS: that's great news. Is
15 there a place in which with the regards to the bills
16 that were heard today or that were mentioned today,
17 do you think that there's something that needs to be
18 added to what we could be doing to help in that
19 transparency and that accountability? And we can
20 talk about that offline. It could be a yes or no. I
21 don't want to--

22 COMMISSIONER STRAUBER: [interposing] No,
23 I mean, at the moment, I don't think so. I mean, I
24 think the legislation has captured some of what I
25

2 think are the most important suggestions and
3 recommendations that we made.

4 CHAIRPERSON HANKS: What actions can the
5 NYPD make to enhance the public awareness and
6 transparency regarding the deployment of new
7 surveillance technologies and associated public
8 comment periods?

9 COMMISSIONER STRAUBER: Well, certainly I
10 think to the extent that they are deploying a new, a
11 distinct surveillance technology, issuing an IUP for
12 that technology provides the maximum sort of public--
13 the opportunity for public input because there is a
14 draft policy issued. As we heard today there's a
15 notice and comment period. The Department then
16 considers that comment and then issues the final
17 report. I think for circumstances where there's an
18 upgrade, it's important that there be an addendum,
19 and I think we've heard about, you know, the
20 Department's view on that, and that they would
21 provide that in a situation where the technology is
22 upgraded. I think these are the best ways under the
23 current framework for the public to understand the
24 technology, and I think the more information that is
25 provided publicly within the limits of protecting

2 what might otherwise-- areas where disclosure might
3 compromise law enforcement is the best way for the
4 public to get some comfort about the nature of the
5 technologies and how they're being used.

6 CHAIRPERSON HANKS: I very much
7 appreciate your testimony, and you know, the briefing
8 on your-- on the report, and so thank you so much.
9 And I'll pass it along to my colleague Chair
10 Gutiérrez.

11 CHAIRPERSON GUTIÉRREZ: Thank you, Chair,
12 and thank you, Commissioner, so much for staying this
13 entire time and for your thoughtfulness in your
14 testimony and certainly in your agency's reporting.
15 I also hope that you take back before the release of
16 your report and certainly all the ones thereafter. I
17 think it is, yes, about the use of devices such as
18 Digidog and K5, but I think for advocates and for New
19 Yorkers and definitely for folks in my community,
20 it's when we're seeing the rollout of these
21 technologies at the cost of making what seems like is
22 proportionate cuts to other social services,
23 agencies, and so yes, I think there is mixed reviews
24 on like the purpose of Digidog, and honestly what the
25 Chief said here today, to me it sounded like fine, it

2 could go upstairs and there were examples where it
3 works, but I think where you hear a lot of the
4 contention is around where releasing all of this
5 equipment and we're saying it's to keep New Yorkers
6 safe, but we're also making cuts to after school
7 programs and to housing programs. So I know that your
8 acute focus as he Commissioner for DOI is -- if this
9 is like of ours specific to the POST Act, but there's
10 a lot more context here, it's still why you hear
11 opposition from advocates. It is about surveillance
12 and it's about transparency, but it's also the
13 agency's ability to kind of roll out what they deem
14 are priorities with very little checks and balances,
15 with very little consultation you heard here with
16 OTI that they need to do it and they're not going to do
17 it. And what I appreciated from your testimony and
18 from the report is they didn't-- but outside of its
19 one piece they did not violate the POST Act, but as
20 the City's premier safety agency, they should be
21 doing a lot more for the purpose of transparency.
22 They should be doing a lot more for the purpose of
23 invoking trust with New Yorkers. So, if any of that
24 is also considered, we would love that. In your
25 testimony, Commissioner, you mentioned that PD has

2 finally agreed to provide an itemized list of
3 surveillance technologies. They have not. What has
4 the wait time been like since?

5 COMMISSIONER STRAUBER: Well, we did make
6 this recommendation in our original report.

7 CHAIRPERSON GUTIÉRREZ: In 22.

8 COMMISSIONER STRAUBER: Which was issued
9 in November of 2022. We have not yet received the
10 list, but I understand that we will receive it. I
11 don't have a specific time frame.

12 CHAIRPERSON GUTIÉRREZ: Gotcha [sic],
13 gotcha, okay. Are there any other key findings from
14 that report which NYPD in your opinion did not, you
15 know, meet the standards of the POST Act, the spirit?
16 I think you said this in your testimony, you
17 appreciated is you know, the POST Act is a very
18 explicit piece of language, but there is a lot more
19 behind that spirit. Are there any other things that
20 you would like to highlight from that report that
21 they didn't do out of the how many recommendations
22 that you made that--

23 COMMISSIONER STRAUBER: [interposing] We
24 had 25 recommendations, so.

25 CHAIRPERSON GUTIÉRREZ: Gotcha.

2 COMMISSIONER STRAUBER: You know,
3 actually, there isn't anything that goes beyond sort
4 of what I already said in my testimony. I mean, I
5 think the focus here and the value, one of the key
6 values that our reports serve is to bring some of
7 this information to the public and make clear where
8 there is more information, more transparency that the
9 Police Department can provide.

10 CHAIRPERSON GUTIÉRREZ: Okay. And have
11 there been any-- have there been any identified
12 changes in how the PD is publishing or updating their
13 IUP since the last report was released?

14 COMMISSIONER STRAUBER: So, I think to
15 the extent that with respect to the IUPs that we're
16 examining for the upcoming report, if there are
17 changes of that nature, we will note those. There's
18 nothing I can point to right now that I can identify
19 as a change in practices, but we will be thinking
20 about that, you know, as we prepare the upcoming
21 draft.

22 CHAIRPERSON GUTIÉRREZ: And does OIG-NYPD
23 have access to all contract agreements and terms or
24 conditions with vendors of surveillance technologies?
25

2 COMMISSIONER STRAUBER: so, one of the
3 things that we requested in our report was that we
4 have those terms and conditions. I do not think we
5 have those at the moment. Now, that doesn't mean that
6 if we make a specific request for those things, in
7 the context of, for example, the upcoming inquiry.
8 I'm not saying we've asked for it and we're not
9 getting it, but as a general matter our proposal was
10 that we receive all of those contracts so that we can
11 review them and see what sort of retention,
12 requirements, and protections those vendors build
13 into their systems, and we do not have those yet.

14 CHAIRPERSON GUTIÉRREZ: Nor have they
15 agreed to provide them.

16 COMMISSIONER STRAUBER: I don't think
17 they've agreed to provide those. But we are-- we do
18 remain as part of our process with the Police
19 Department, we are in a very consistent regular
20 dialogue with them about all of our outstanding
21 recommendations, and I'm optimistic now that we're
22 getting the itemized list that perhaps there'll be an
23 opportunity to get some more of this information.

24 CHAIRPERSON GUTIÉRREZ: Great. My last
25 couple questions, Commissioner, are related to the

2 public process of amendments to IUPs. I know you
3 said, I know the Chief said, like these public-- this
4 public engagement process or public comment process
5 exists and considerations are made. Is DOI present
6 for these, like, public engage--

7 COMMISSIONER STRAUBER: [interposing] We
8 are not part of that process.

9 CHAIRPERSON GUTIÉRREZ: Okay.

10 COMMISSIONER STRAUBER: My understanding
11 is there's public comment, public-- to the extent the
12 public has input. There are members, I believe, of
13 the legal department at the NYPD to consider that
14 input and then work on the policies accordingly, but
15 we have not been part of that process.

16 CHAIRPERSON GUTIÉRREZ: I'm just
17 interested in the realities of how like how much of
18 the public comment they're integrating into their
19 IUPs. I believe that-- the advocates that are-- that
20 have been in support of the POST Act since it was
21 first introduced years ago, obviously I think their--
22 this is on their google alerts. They're following
23 this. They're showing up. But you know, the sake of
24 having, you know, saying that there's a public
25 comment period for the sake of it and having none of

2 it be realized in the IUP, for example, and I'm not
3 saying that that's happening. I'm just curious if you
4 have an understanding of how much of that comment--
5 of the public's comment is integrated into their
6 amendments of IUPs.

7 COMMISSIONER STRAUBER: I know we made
8 some reference of this in our 2022 report because we
9 looked at the volume of comments, and there were
10 actually a couple of changes that were made that
11 relate-- that it did relate to the comments that came
12 in, but I'm not in the position to sort of give you
13 real sense of, you know, that the extent of the
14 changes that are made based on the public comments
15 sitting here today. I just don't know.

16 CHAIRPERSON GUTIÉRREZ: Okay. Thank you,
17 Commissioner. Do we have any questions from members?

18 CHAIRPERSON HANKS: Yes, we do. Council
19 Member Holden?

20 COUNCIL MEMBER HOLDEN: Thank you,
21 Chairs. Thank you, Commissioner, again for staying.
22 And just a couple of questions on-- well, NYPD was
23 really against Intro 1207. They said it was vague.
24 Do you consider-- did you find anything vague in
25 1207?

2 COMMISSIONER STRAUBER: Well, I think
3 perhaps the language-- if we were working with you on
4 the language, there's a reference to the fact that
5 even if there's overlap with capabilities and
6 functionalities of other technologies, there still
7 needs to be a distinct IUP. And I think we could in
8 future discussion maybe have some ideas about that
9 language so that it's clear-- if this is the
10 Council's view I think this is our view, that if
11 there are substantial overlap with the functionality
12 of another technology, then it's not our position
13 that there needs to be a separate IUP. It's where
14 you're really talking about something distinct, and I
15 think this is a line drawing exercise, but working on
16 language that sort of captures that perhaps a little
17 bit better is something that we'd be happy to
18 contribute to.

19 COUNCIL MEMBER HOLDEN: Since we were
20 talking about the Digidog, let's say that your
21 concerns would be if they added something else to it,
22 some other-- that they don't have now. I don't know
23 what exactly they have on the dog. You know, for
24 instance, tear gas, if they added that, if they added
25 something else, that would be a concern, or would it?

2 Because I did buy the idea that because the dog can
3 climb up the stairs-- you know, R2D2 couldn't, right?
4 I mean, there's technology that we need sometimes
5 because there are obviously stairs to climb, and
6 that's a valuable robot actually to do that. So what
7 else would be concerning to the dog, really? It has
8 no weapons on it. It maybe has cameras, obviously,
9 but what else would be-- like, let's say for
10 instance, in your studies?

11 COMMISSIONER STRAUBER: Right, so I can't
12 get too far ahead of myself here, because we're
13 literally in the process of working on a report on
14 this, but I just want to be clear that I don't think
15 the-- I think I share your view that to the extent
16 technology serves a valuable law enforcement purpose,
17 it's a good thing, and I'm not concerned about the
18 technology itself. I think what we're saying is, if
19 the Digidog is captured and described in the
20 situational awareness camera IUP, does that document
21 really tell the public enough about Digidog, or are
22 there features of Digidog that are kind of not made
23 clear to the public because Digidog is included in an
24 IUP that's really focused on situational awareness
25 cameras. And Digidog might be a camera, but it might

2 be more than that. And what we'd be looking to say
3 is, if there's more than that, is that sufficiently
4 disclosed.

5 COUNCIL MEMBER HOLDEN: Right, but again,
6 it's what you just mentioned, is that if we give too
7 much information on the dog, then the bad guys would
8 know how to maybe defeat it, or what it could do, or
9 throw a blanket over it. You know, there's a number
10 of things that I think we don't want to give away.

11 COMMISSIONER STRAUBER: I think there's a
12 balance there, absolutely.

13 COUNCIL MEMBER HOLDEN: Yeah, and that's
14 the key here, because-- and that's why you're
15 important and drafting new-- you know, obviously, the
16 POST Act, they actually-- you said yourself they were
17 within the POST Act, right?

18 COMMISSIONER STRAUBER: That's what we
19 found for the most part.

20 COUNCIL MEMBER HOLDEN: for the-- okay,
21 for the most part. But your recommendations where
22 they weren't, they rejected that?

23 COMMISSIONER STRAUBER: They did, yes.

24 COUNCIL MEMBER HOLDEN: Okay.
25

2 COMMISSIONER STRAUBER: Although we've
3 had some progress now on receiving this list of
4 technologies which was one of our recommendations,
5 and we're going to continue to have a dialogue with
6 them and hope that we can make some more progress.

7 COUNCIL MEMBER HOLDEN: Great. Thank you,
8 Commissioner. Thanks so much.

9 CHAIRPERSON HANKS: Council Member Brewer?

10 COUNCIL MEMBER BREWER: Thank you very
11 much. I am-- I know you mentioned this dog and the
12 robots, but are you not also looking-- because I have
13 to say I'm more interested in the facial recognition,
14 drones, and other kinds of surveillance. Are they
15 also part of your discussion?

16 COMMISSIONER STRAUBER: So, we addressed
17 facial recognition in our 2022 report.

18 COUNCIL MEMBER BREWER: And you got
19 answers on that? I mean your recommendations.

20 COMMISSIONER STRAUBER: Yeah, we made--
21 actually, I was just looking back at the report. We
22 don't-- our recommendations are not specific to
23 facial recognition, but we did-- but actually, that's
24 not correct. We did make recommendations as to
25 facial recognition, and some of those have been taken

2 up in the proposed legislation here, and we're
3 appreciative of that. So, we recommended that there
4 be an auditing process and that there be a published
5 policy and procedure relating to how the conduct of
6 facial recognition work is done. So we did address
7 that in 2022. That's not something we're currently
8 planning to address in the upcoming report. In some
9 future report, of course, we could take a look at it.
10 We're also, as far as I know, not specifically
11 focused on drones. Again, that is something that we
12 could look at in the future.

13 COUNCIL MEMBER BREWER: Okay, because
14 what you're saying on the facial recognition is that
15 the recommendations were not necessarily abided by,
16 but the legislation that's proposed-- but the Police
17 Department should have done it, not the City Council.
18 That's why I'm confused.

19 COMMISSIONER STRAUBER: Well, we made
20 recommendations to the Police Department. It was
21 certainly within their power to do those things even
22 if they--

23 COUNCIL MEMBER BREWER: [interposing]
24 Yeah, that's what I'm saying.

2 COMMISSIONER STRAUBER: were not required
3 by the POST Act. For the recommendations, obviously,
4 we're always grateful when the City Council agrees
5 with some of the recommendations we've made and
6 considers, you know, making those part of
7 legislation. That's what's happened here with the
8 facial recognition recommendations.

9 COUNCIL MEMBER BREWER: Okay. And are
10 there other technologies popping up that you're aware
11 of-- obviously, we didn't know about the dogs until
12 recently-- that should be considered in the future?
13 Do you have any suggestions about that, or?

14 COMMISSIONER STRAUBER: You know, I can
15 certainly say, although I don't have the complete
16 list of them here right now, that in addition to the
17 robot and the dog, we are looking at a couple others
18 at the moment, and those will either be in a report
19 in the first quarter or a subsequent report. So we
20 are certainly alert and watching for these things as
21 they're announced.

22 COUNCIL MEMBER BREWER: [inaudible] even
23 things like cameras, because one could track from
24 somebody from New York to Florida with cameras
25 easily, according to NYPD. Is that something that

2 comes up under POST Act, or that's not covered
3 because it's not--

4 COMMISSIONER STRAUBER: [interposing]
5 Well, if you're referring-- there's a technology
6 called License Plate Readers or LPRS, and I think
7 that's probably what you're referring to when you say
8 like to the extent that numerous states have that
9 kind of technology--

10 COUNCIL MEMBER BREWER: [interposing] Yes.

11 COMMISSIONER STRAUBER: you can track
12 someone who's driving from point A to point B. We
13 did look at LPRs in connection with our initial
14 report, and we had some recommendations relating to
15 being more specific about how long that data is
16 retained and that kind of thing. So we have looked
17 at those.

18 COUNCIL MEMBER BREWER: Do you have
19 access to all contract agreements and terms with
20 vendors or surveillance technology? Is that
21 something that is both part of your request and
22 answered? A big focus on contracts.

23 COMMISSIONER STRAUBER: We have not
24 received all of the contracts for all the
25 technologies. That was one of our recommendations,

2 and we have not received those. We're going to sort
3 of restart that dialogue now that we're getting the
4 itemized list of technologies. I think it would make
5 sense for us to have the vendor contracts that go
6 along with them, to the extent that they are sourced
7 from the outside, which many of these technologies
8 are, to the point that you were making earlier.

9 COUNCIL MEMBER BREWER: So, in your first
10 report, and I should know this, did you ask for that
11 or only now are you asking for these contracts?

12 COMMISSIONER STRAUBER: No, we asked for
13 that. That was one of the recommendations in our
14 first report.

15 COUNCIL MEMBER BREWER: And you did not
16 get it.

17 COMMISSIONER STRAUBER: WE did not get it.

18 COUNCIL MEMBER BREWER: That's a problem.
19 Thank you very much.

20 CHAIRPERSON GUTIÉRREZ: Okay, and with
21 that, thank you so much, Commissioner. We are
22 excited for the release of the next report. We'll do
23 this all over again next year, hopefully. And I also
24 just want to thank OTI. Stacey [sp?] thank you so
25 much for staying. And this concludes, right, the

2 agency portion and I think we can go straight ahead
3 to the public testimony. No breaks. Power through
4 everyone.

5 COMMISSIONER STRAUBER: Thank you.

6 CHAIRPERSON GUTIÉRREZ: Thank you,
7 Commissioner.

8 COMMITTEE COUNSEL: Public testimony
9 we're going to start with Michael Sisitzky from New
10 York Civil Liberties Union, Jerome Greco from Legal
11 Aid Society, and Nina Loshkajian from STOP. We're
12 going to make three minutes available for individuals
13 to testify, and you're free to submit written
14 testimony as well. Thank you.

15 CHAIRPERSON GUTIÉRREZ: You can begin
16 when you're ready.

17 MICHAEL SISITZKY: Good afternoon. Thank
18 you, Chair. My name is Michael Sisitzky, Assistant
19 Policy Director with the New York Civil Liberties
20 Union. So we'll be submitting full written comments
21 for the record. I'll focus my comments today on a
22 few things that we observed with the overall
23 compliance or lack thereof with the POST Act and the
24 NYPD's policies, and also address some points that
25 come up from the discussion earlier and hopefully

2 clarify some issues for the Council. So I just
3 wanted to start with the big picture. the POST Act
4 was a first step towards getting a better
5 understanding of the NYPD's approach to surveilling
6 New Yorkers, and it was really not that much of an
7 ask. This was basic transparency. This was a really
8 clear and simple assignment. And it's an assignment
9 the NYPD failed. When we reviewed the NYPD's POST
10 Act policies when they were first published, the
11 drafts, in 2021, you know, we observed so many issues
12 in terms of the Department's attempt to evade those
13 minimal transparency mandates in the Act. This
14 included inaccuracies and misleading statements,
15 omissions that occurred throughout these policies. So
16 I want to touch on a few things. Yeah, there were
17 some conversation earlier around whether the
18 Department using artificial intelligence or machine
19 learning. In the first draft of the NYPD's policies
20 pretty much across the board, there was a statement
21 that the department does not use artificial
22 intelligence or machine learning in those policies.
23 When it was pointed out to the NYPD in our comments
24 and comments from many of our partners that in fact
25 facial recognition is reliant on those very

2 processes, that shot spotter which the NYPD operates
3 has an entire section devoted to the technology's
4 artificial intelligence and machine learning
5 capabilities on their website, the NYPD simply just
6 removed any references to artificial intelligence and
7 machine learning from their policies going forward,
8 basically saying, well, there's not an accepted
9 industry-wide definition, so we're just not going to
10 even acknowledge these capabilities at all. There
11 were major issues in terms of the Department's
12 approach to considering the potential disparate
13 impact from these policies which was the crucial
14 reason that communities were pushing for the POST Act
15 in the first place, to understand how these polices
16 were actually impacting communities. the Department
17 basically used the same boiler plate, copy and paste
18 language, saying that there were no disparities in
19 any of their uses of the technologies, and claimed
20 that in their interpretation they were only required
21 to consider whether the policies themselves and not
22 the underlying technology was actually capable of
23 producing disparities. But to the extent that these
24 policies were supposed to contain the rules and
25 procedures for how these technologies are used in

2 practice, it's very clear that the council's intent
3 all along was to consider the ways these technologies
4 could be weaponized against communities of color.

5 And you know, the copy and paste language that went
6 into this, there was talk earlier about how it could
7 be confusing if the Department were to do a less
8 boiler plate approach and not repeat the same kind of

9 clauses over and over again. it's really the case

10 that, you know, the-- it's actually more confusing

11 for the public to understand what these technologies

12 are and how they operate and what their impact is,

13 and to the extent that the Department was claiming

14 that this is providing more clarity and more

15 information for the public in their initial draft

16 which, you know, they corrected. Their disparate

17 impact policies on unmanned aerial systems actually

18 included a reference to a different technology,

19 because they had been simply copying and pasting. So

20 this is a law-- I know my time's expired, so I'll

21 wrap up. This is a law that the NYPD has never had

22 any real intention of implementing and complying

23 with, which is why it's really incumbent on the

24 council to take further action. We support the

25 recommendations from the Office of the Inspector

2 General and that are contained within the bills
3 before the Council and it's really critical that the
4 Council actually legislate on this. We know the NYPD
5 has a long track record of rejecting OIG
6 recommendations. We don't anticipate that without
7 Council action they will improve their practices, and
8 I want to just emphasize that this is also a point
9 where-- you know, again, the POST Act was the first
10 step towards transparency, but it was also a first
11 step towards further regulations and restrictions on
12 NYPD activities. The transparency is an important
13 goal but it is not the goal in and of itself. We
14 need to be using these reports, this information to
15 better regulate and restrict and ban certain
16 practices by the NYPD, including imposing bans on
17 things like facial recognition and getting a better
18 handle on exactly how New Yorkers are policed and
19 surveilled. Thank you.

20 CHAIRPERSON GUTIÉRREZ: thank you.

21 NINA LOSKAJIAN: Thank you. Good
22 afternoon Chair Gutiérrez, and thank you for
23 organizing this important hearing. I'm a staff
24 attorney at the Surveillance Technology Oversight
25 Project, and we are here to support Intros 1207 and

2 1193 and to continue to work with your office
3 hopefully to amend them into the strongest versions
4 possible. The POST Act was an essential first step,
5 as Michael noted, in gaining greater transparency
6 over NYPD's use of repressive surveillance against
7 black and brown New Yorkers. While it was just a
8 first step, it was still a landmark bill, because it
9 re-asserted the Council's indispensable role in
10 overseeing NYPD operations. The Council must now
11 again reassert its authority to ensure that the bill
12 it fought so long to implement is not totally
13 ignored. Three years since its passage, it is clear
14 the Department has blatantly disregarded the law's
15 requirements. Its IUPs consist largely of boiler
16 plate language not specific to each individual
17 technology. And I just want to pick up on something
18 that Michael noted, the Department today described
19 having to do additional IUPs as something that would
20 be-- or cause repetition and confusion. What is
21 repetitive and confusing is their current approach to
22 IUPs. That's not the reality of what would change by
23 requiring additional IUPs. And this failure to comply
24 has detrimental consequences. Because of NYPD's
25 secrecy, we don't know what private contractors get

2 access to our info. We don't know how much disparate
3 harm to vulnerable communities the NYPD is acceptable
4 in its surveillance tools, and that's incredibly
5 disturbing especially given the example Council
6 Member Stevens cited today of the gang database being
7 99 percent black and Latinx. We support the language
8 that was taken directly from the OIG's
9 straightforward recommendations in their Department--
10 in their report, sorry. These recommendations
11 reflected clearly how the Department can and should
12 change its practice to adhere to the law. NYPD's
13 surveillance arsenal is expanding rapidly in
14 violation of the POST Act. Mayor Adams is constantly
15 rolling out new spyware that costs the City millions
16 of dollars, and as you highlighted, at the same time
17 cutting back funding from crucial services. To truly
18 protect New Yorkers, the City Council must fully
19 outlaw discriminatory surveillance technologies,
20 including facial recognition, fake police social
21 media profiles, drones, and other spyware, but while
22 we wait for such bans, the very least New Yorkers
23 deserve is transparency. We urge the council to
24 listen to advocates and the OIG in taking urgent
25 steps to ensure the NYPD follows the rule of law.

2 And just one final note, is that when the original
3 POST Act was being considered, the NYPD was so
4 adamant that this would-- the sky would fall. It
5 would be a road map to terrorists, and in their
6 testimony today very interestingly they said that the
7 POST Act has not impeded its counterterrorism
8 efforts. So it's just proof that the NYPD will
9 continue to say the sky is falling whenever it is
10 held to the lowest standard of accountability and
11 that can't be reason to not hold their feet to the
12 fire.

13 CHAIRPERSON GUTIÉRREZ: Thank you. That
14 was great, yeah, absolutely.

15 JEROME GRECO: Thank you for having me
16 here today. I'm Jerome Greco. I'm the Digital
17 Forensic Supervising Attorney at the Legal Aid
18 Society. I'm going to address two things that I
19 think the Legal Aid Society particularly well-quipped
20 to address. The first is related to the contracts
21 that the NYPD has kept secret. There was a lot of
22 testimony here today that is inconsistent with what I
23 know for a fact to be true based on hearings and
24 lawsuits that are still ongoing. So, the NYPD along
25 with the DOI, the Comptroller's Office, the Mayor's

2 Office of Contract Services, Office of Management and
3 Budget, and the Law Department had an agreement for
4 13 years that allowed them to keep secret a lot of
5 these contracts. I'm talking about thousands of
6 pages of contract. After the Post Act passed, the
7 Comptroller's Office at the time withdrew from that
8 agreement, but it is my understanding that the other
9 agencies are still part of it in order to keep secret
10 these-- all these different surveillance contracts.
11 We're able to obtain many pages, again, thousands of
12 pages, from the Comptroller's Office of these
13 contracts, but as part of that agreement, the
14 Comptroller was only allowed to hold onto copies that
15 the NYPD had redacted. And so some of these, we
16 don't even know the names of the companies and how
17 much money the NYPD was giving to them from tax payer
18 money. We subsequently sued the NYPD [inaudible]
19 Article 78 which we recently court ordered-- ruled in
20 our favor, and now the NYPD is appealing it. so when
21 they sit here saying we don't know what you're
22 talking about about secret contracts, they're
23 literally in active litigation with us to prevent us
24 from accessing copies of those contracts to even find
25 out the names of the vendors. So it's baffling for

2 them to say that, and frankly have the gall to say
3 that. related to the facial recognition technology,
4 they keep referring it to this NIS [sic] study, which
5 by the way they never actually cite anywhere, but
6 they allegedly gave the OIG-NYPD and they used this
7 to say that this human process that they have proven
8 that this facial recognition is okay, that it's not
9 the problem we think it is. however, the OIG-NYPD
10 report said, OIG-NYPD reviewed that study and
11 concluded that it does not support NYPD's claim that
12 human observation can remedy erroneous software
13 matches. In fact, to the contrary. The study does
14 not address human observation except to say that the
15 interaction with machine and humans beyond the scope
16 of this study, as is human efficacy. So they're
17 citing to a study that literally does not say what
18 they say it says in order to justify what they're
19 doing. And then the reality of it is that they are
20 just compounding bad identification procedures on top
21 of bad identification procedures, ones which would
22 never be admissible in court, in order to justify an
23 investigation in which then there is zero procedure
24 for what happens after that. It's not, can you stop
25 someone's car based on a facial recognition match?

2 Can you stop them on the street? What [inaudible]
3 level does that get? What level of interaction can
4 you have with somebody? Can you go to their job and
5 interrogate them? There's zero procedure, zero rules
6 from the NYPD about that. Not to mention, that this
7 investigative lead that they keep referring to. What
8 they actually do is they look at that person's
9 history and they send it to-- they send a photo to an
10 officer who's previously arrested him and says, hey,
11 do you recognize this guy? Why do you think that
12 officer thinks he's getting that picture? Because he
13 must know who that person is. He has no connection
14 to the investigation otherwise. He says, yeah, I
15 know that person. I previously arrested him. That's
16 what then they're going to make an arrest. That's
17 not a legitimate investigation, and for them to say
18 it's only an investigative lead as if it doesn't
19 direct their investigation and that they don't
20 essentially launder it through this fake
21 identification procedure is ridiculous. So, Legal
22 Aid Society supports strengthening the bills that
23 have been presented, particularly 1193 and 1207, and
24 we hope the Council will take it up and [inaudible].

2 CHAIRPERSON GUTIÉRREZ: Thank you. Thank
3 you for your testimonies. I have it here. Can I
4 just ask one question related to the IUP process?
5 Because I think, obviously some of the bills are
6 trying to strengthen kind of how they amend these
7 IUPs, what they're including, and to specify what
8 they're used for, these specific technologies. What
9 is this like-- what is the public testimony process
10 like, because I'm very curious if, obviously, they're
11 just taking public record of it, and like, I would
12 love to see where public testimony is integrated into
13 some of these amendments. I'm not sure if they're
14 happening. What can you say in your experience of
15 these-- of this like, public portion?

16 JEROME GRECO: So, I could say that it's
17 only happened once so far, and that when they--

18 CHAIRPERSON GUTIÉRREZ: [interposing]
19 There's only been one public portion, but they said
20 today they've made various amendments?

21 JEROME GRECO: Right, but those
22 amendments have not been subject to public
23 commentary--

24 CHAIRPERSON GUTIÉRREZ: [interposing]
25 That's right. That's right, only the new ones.

2 JAMES GRECO: Right, and so only when
3 they initially released the 36 was there any public
4 commentary period.

5 CHAIRPERSON GUTIÉRREZ: The one time.

6 JAMES GRECO: And for-- I know for us, we
7 submitted close to 50 pages of comments which seemed
8 mostly to have been ignored. I think other people
9 felt similarly. I do know for example, when certain
10 issues were pointed out, I think Michael was talking
11 earlier about their saying artificial intelligence
12 and machine learning weren't being used, and they
13 were called out on that. Instead of defining that or
14 fixing it, they just removed that statement, which
15 seems to be their-- the path of least resistance.

16 CHAIRPERSON GUTIÉRREZ: Thank you.

17 COMMITTEE COUNSEL: Thank you for your
18 testimony. Next, we'll hear from Jonathan Lamb with
19 Amnesty International, Ivey Dyson with the Brennan
20 Center of Justice, and Elizabeth Vasquez from
21 Brooklyn Defender Services.

22 ELIZABETH VASQUEZ: Good afternoon. My
23 name is Elizabeth Daniel Vasquez, and I direct
24 something called the Science and Surveillance Project
25 at Brooklyn Defender Services. My job every day is

2 to work with criminal defense attorneys, family
3 defense attorneys, immigration attorneys, housing
4 attorneys to understand the ways in which the NYPD is
5 using technology, the ways in which they are
6 surveilling our clients, and the information that
7 they are collecting. When the POST Act passed, we
8 felt like this was going to be an incredibly positive
9 step towards getting some more transparency around
10 what has always been an incredibly opaque system of
11 buying, procuring, implementing, and rolling out
12 technology that we had no notion of until it would
13 show up as potentially a set of letters in discovery,
14 and then we would be left to be like, what is that,
15 and try to figure out what's going on. When the POST
16 Act Impact and Use Policies came out, what we were
17 left with was 36 repetitive statements that didn't
18 give us much insight, but there were a couple of
19 things that I think are worth flagging here. I agree
20 with everything that folks talked about in the last
21 panel, but what I want to focus on is what we did
22 actually learn from what they said. So the first
23 thing is, today they chose to focus on the wiretap
24 act and to talk to the Council about the requirements
25 for minimization that were in that particular

2 provision. When you look at their IUPs, 36 of them,
3 only four do they say that they require court
4 oversight in order to use those technologies. So
5 where, we're talking about aggregate technologies, so
6 many more than just the 36, and what we're getting is
7 four that would have required court oversight. This
8 should cause us pause. It should also make us think
9 about the incredibly important role of the Council in
10 reigning them in. because if they are saying to you
11 we do not have to go to the criminal court to ask for
12 permission to do these things, then you are the only
13 ones that stand in the way of them and the
14 information collection that they are engaged in. the
15 second thing that we learned from these Impact and
16 Use Policies, what they actually did perhaps
17 accidentally, track the way that they were sharing
18 information across systems within those policies.
19 And so to your question, Council Member Gutiérrez,
20 when you were asking about the Domain Awareness
21 System and they kept saying, no, no, the Domain
22 Awareness System is not a surveillance tool, it's
23 just ingesting everything. That was revealing because
24 it's not just the Domain Awareness System that is
25 doing that, and when you look at all 36 policies,

2 what you start to see is that the technologies are in
3 important in the sense that they are grabbing data
4 streams, but where are those data streams going needs
5 to be the next set of questions that we ask. And
6 they have done everything they can to not come to
7 accountability on the answer to that particular part
8 of this question. Because when they say we're not
9 using machine learning, or we're not using artificial
10 intelligence, what they're really trying to obscure
11 is that they have collected all of the data in order
12 to act upon it. They act upon it using machine
13 learning products. They act upon it using their own
14 search capabilities within the Domain Awareness
15 System, but they are not just collecting this data
16 for no purpose. And so it is critically important
17 that the Council start to think not just about
18 banning individual technologies, but about fully
19 reckoning with the way that the NYPD obtains the
20 data, how long they are allowed to keep it, and what
21 purposes they are entitled to put it to. I'll stop
22 there.

23 CHAIRPERSON GUTIÉRREZ: Thank you.

24 IVEY DYSON: Good afternoon Chair
25 Gutiérrez. My name's Ivey Dyson. I serve as Counsel

2 at the Brennan Center for Justice in our Liberty and
3 National Security Program. As part of our focus on
4 government oversight and accountability, we advocated
5 for the passage of the POST Act, but unfortunately,
6 the NYPD, as you know, has consistently evaded the
7 Act's disclosure requirements while continuing to
8 expand its arsenal of surveillance technology.

9 Members of City Council have introduced two bills
10 aimed to strengthen the POST Act and which we
11 support, but we believe there are additional common
12 sense changes that the Council should make to ensure
13 that the NYPD surveillance does not go unchecked.

14 So, to date, the NYPD has used generic language in
15 its POST Act disclosures to explain how it shares
16 surveillance data with outside actors, such as
17 federal immigration agencies and city housing
18 authorities. City Council must require the NYPD to
19 share more information on how external agencies
20 access its surveillance data and whether there are
21 restrictions on how that data is used, such as how
22 long it can be kept, whether it can be copied, and if
23 any other entities can access surveillance data that
24 NYPD has transferred to external agencies. As put
25 forth by the NYPD Inspector General, the police

2 should also maintain an internal tracking system
3 recording every instance in which the Department
4 provides an external agency with surveillance data,
5 and the NYPD must publish any known safety hazards
6 for each surveillance technology it uses. And
7 finally, the City Council must address the NYPD's
8 failure to provide meaningful information on the
9 potential disparate impacts of its surveillance
10 technologies. The NYPD has a history of
11 discriminatory surveillance, and the Department
12 continues to use facial recognition technology that
13 has led to wrongful arrests of black Americans across
14 the country based on racialized errors. The NYPD
15 must provide more information on the disparate
16 impacts of the surveillance technology it uses,
17 specifically any variations in accuracy of the
18 technology based on a characteristic protected by New
19 York City Human Rights Laws such as race or religion.
20 I also want to highlight something that you brought
21 up earlier, Chair Gutiérrez, about the NYPD's open
22 FOIL request related to surveillance and activities
23 and, you know, social media monitoring activities.
24 The Brennan Center filed FOIL requests in 2020
25 related to the NYPD's use of social media monitoring

2 and social media monitoring tools, and I know there
3 are other advocates who are here in the room who have
4 filed many FOIL requests related to surveillance
5 policing and have open request that have still been
6 unanswered or have had to file an Article 78 petition
7 for every single question because they've not
8 received adequate information. And so this is
9 another reason why POST Act compliance is so
10 important so that we have an actual mechanism where
11 the NYPD has to be held accountable for the
12 surveillance technology it uses. And the City
13 Council passed the POST Act in response to public
14 demand for greater police accountability, and it must
15 now strengthen the law to ensure the police can no
16 longer evade the transparency that New Yorkers
17 deserve. Thank you.

18 JOHNATHAN LAMB: Good evening Council.

19 Thank you for giving me the opportunity to testify on
20 the use of facial recognition technology in New York
21 City. My name is Johnathan Lamb. I'm a freshman at
22 Cornell University. I was born and raised in Jackson
23 Heights, Queens, and I'm here today as a student
24 activist leader, a part of Amnesty International Ban
25 the Scan Taskforce in New York. Our taskforce work

2 has focused on the use of NYPD's use of face
3 recognition technology, its abuse against
4 marginalized communities, and its attack against our
5 common privacy rights. Amnesty International
6 launched an ambitious effort called Decode
7 Surveillance NYC. This effort mobilized thousands of
8 digital volunteers to find and categorize CCTV
9 cameras throughout this city. In addition they worked
10 and investigated these findings with data scientists,
11 geo-photographers [sic], 3D modifiers to analyze this
12 data, and as a result, the results were very
13 shocking. The taskforce found that the NYPD has been
14 using face recognition technology in over 2,022 cases
15 from 2016 to 2019, half of which came from 2019
16 alone, and this issue has affected marginalized
17 communities in New York City the most. Through
18 analysis and research we also found that areas in
19 communities of color that have seen brutal policing
20 tactics are likely to be more exposed to invasion
21 facial recognition technology. When looking at the
22 Bronx, Brooklyn and Queens, the most diverse boroughs
23 in the city, our data shows that communities of color
24 have the highest concentration of facial recognition
25 CCTV cameras, even when Black Lives Matter protests

2 were occurring during the pandemic, protesters risked
3 high levels of exposure to face recognition
4 technology. Only two months ago we saw that face
5 recognition technology were finally banned in New
6 York State School statewide. As someone who went to
7 the New York City K-12 public school education system
8 and who went to a school that was over-policed, it's
9 time that we look into facial recognition
10 technologies as a broader community so our community
11 members, especially BIPOC youth feel safe and
12 protected. With the rise in protests and public
13 demonstrations due to current political conflicts, it
14 is so important that we're protecting youth activists
15 who are participating in these actions and basic
16 first amendment rights. According to the New York
17 Civil Liberties Union, there are plenty of research
18 that demonstrated how inaccurate facial recognition
19 are, and there's a risk of cooperation between ICE
20 and the NYPD. as the son of Vietnamese refugees and
21 coming from Jackson Heights, a predominant immigrant
22 community with a high immigrant population, it so
23 vital that we are re-envisioning public safety that
24 does not foster xenophobia and discriminatory
25 practices towards community members. We need to

2 enact 1207 and 1193 in order to hold the NYPD
3 accountable for their usage of facial recognition and
4 transparency. There is much-needed urgency-- reforms
5 are needed for the POST Act. The usage of facial
6 recognition technology is not a political issue, but
7 it's a human rights and public safety issue. Thank
8 you.

9 CHAIRPERSON GUTIÉRREZ: Thank you all so
10 much for sticking around and testifying. Appreciate
11 you all. Thank you.

12 COMMITTEE COUNSEL: Thank you all for
13 your testimony. We're going to do a combination
14 panel for folks on Zoom as well. We'll hear from
15 Towaki Komatsu, Raul Rivera, and Andrew. We also
16 have online-- read out your names so you're ready,
17 Christopher Leon Johnson. Whoever wants to go first
18 may go ahead. Christopher Leon Johnson, are you
19 available? Oh, there you are. Christopher?

20 RAUL RIVERA: Good afternoon, my name is
21 Raul Rivera. I'm a New York native, TLC driver
22 advocate, and I just want to get a quote out of the
23 way before I forget it, because I kind of forget a
24 lot. Humans first, technology second, today,
25 tomorrow, forever. I repeat, humans first,

2 technology second, today, tomorrow, forever. So,
3 we're concerned about the NYPD, and so am I. We
4 don't fully trust them, but we have to say that we
5 need cops in this city. New Yorkers need cops in the
6 city, and when we have elected officials who are
7 voted in, and just because you're voted in, that
8 doesn't automatically make you a leader, because I
9 don't see all you Council Members as leaders. We do
10 have some that are, and we have others that are not.
11 When we have our-- and that's not to say that New
12 Yorkers agree with me, but there's a lot of people
13 that do see each and every one of you as leaders, and
14 if you going to say defund the cops, that hurts New
15 Yorkers. That hurts a lot of people. That hurts the
16 NYPD. And when we have a Public Advocate who can't
17 stand the police, that's a big problem. When we have
18 Council Members that call for the abolishment of
19 cops, that's a big problem. Maybe reform, but not
20 abolishment. We need cops in this city. I don't
21 know if you guys know, but Jumaane Williams lives in
22 an Army base. Jumaane Williams, the Public Advocate,
23 he lives in an Army base. He's well-protected. Us
24 New Yorkers are not. And when you say defund the
25 cops, you are hurting New Yorkers. So we say, that

2 if you want to be a true leader, you do not do that.

3 That's what we ask. We start with common sense

4 stuff. Me, I'm a lover of technology, but we put

5 humans first, technology second, today, tomorrow,

6 forever. We ask our Council Members to stop saying

7 defund the cops, because when you do that you're

8 telling people they can go in the stores and take

9 whatever they want, to disobey the law, to ignore the

10 cops, to disrespect the cops. I'll leave it there.

11 Thank you.

12 CHAIRPERSON GUTIÉRREZ: Thank you.

13 COMMITTEE COUNSEL: Thank you for your

14 testimony. Looks like we got the gentleman online,

15 so we're going to turn to him before passing it off

16 back to here, okay? So, Christopher Leon Johnson,

17 you may begin.

18 CHRISTOPHER LEON JOHNSON: Alright,

19 what's up everybody? My name is Christopher Leon

20 Johnson on the record. Thank you, Chair Gutiérrez,

21 be on the-- for sticking with us for all this time.

22 Hope you have a happy holiday through the end of the

23 year. I'm here to make this clear, personally, you

24 know? I appreciate the committee. I understand how

25 the NYPD they was dodging, ditching and dodging us

2 the voters, the constituents, because they don't want
3 to really answer why they're spying on New Yorkers.
4 It's just not just the stuff that they're doing with
5 the fake social media accounts, and the over-the-top
6 cameras and body cameras and all the type of-- to
7 surveil us. Not only hurts minorities, it hurt
8 everybody. It hurts every race, every creed, every
9 culture. We just can't make it just about black and
10 Latino and gay people and Asian people. Got to be
11 about all people, including white people. So
12 everybody get affected by the body cameras and all
13 the cameras. What I believe that should happen, that
14 should start happening more is that there should be
15 more real transparency of how these-- about how
16 obtaining the footage of interactions with police. I
17 know that there's a lot of instances of that got a
18 FOIL request, and the NYPD actually rejects the FOIL
19 request, and we need to really need to start making
20 it more hard for the NYPD to-- and help with the--
21 and the NYPD Law Department to rig the cameras and
22 destroy footage and edit footage. If they-- the
23 footage be transparent for all of us to see, if it
24 gets out there like that, you know, that's what
25 should be happening a little more, with the spying--

2 with the cameras and with the footage. Yeah, we need
3 to stop this surveillance on people. I think it's
4 stupid, and it's not transparent at all. The City--
5 I know the problem is that, you know, like I said we
6 have the City Council, you know, they have their
7 hearts and their intentions in the right place of
8 trying to stop this stuff with spying on New Yorkers,
9 but the real political support is not there, because
10 a number of these Council Members, and we all know
11 who they are, they're scared of the police union.
12 All they care about is pandering to the police unions
13 and try to keep their endorsements, which I think is
14 kind of stupid, because the endorsements of the PBA
15 are not even that effective in New York City, you
16 know. I don't-- it's like-- the rate of success with
17 a PBA endorsement is like abysmal. Even Marjorie
18 Velazquez who had that endorsement, she lost to
19 Chrissy Martimoro [sp?] in the general election even
20 with the PBA endorsement. So I don't get why that,
21 you know, this stuff-- you know, we need more
22 transparency with the NYPD and, you know, bills like
23 this, stuff like this need to be heard a little more
24 often. I wish there was more people that was
25 courageous enough to be here on here and speak

2 against this spying, but I understand that people
3 scared of being doxed by the NYPD, and help of their
4 little snitches all over social media and on the
5 streets. But I appreciate you, Jennifer Gutiérrez,
6 for being real cautious with the panels today with
7 the online zoom, that you privatized everything, you
8 didn't put any names out there in the panels. I
9 appreciate it. I understand. But going forward,
10 like I said, we need like more support with this
11 stuff. People need to come out more and testify
12 other than just us three and the legal people. Shout
13 out to all the non-profits [inaudible] Legal Aid,
14 STOP spying, all these other nonprofits that are
15 trying to fight this situation. We need more people
16 to come out there and testify this stuff.

17 SERGEANT AT ARMS: Time has expired.

18 CHRISTOPHER LEON JOHNSON: [inaudible]
19 I'm sorry. A few more seconds. Stop being scared
20 and come out and testify, and we need to stop spying
21 on New York City, and stop these rats [sic] in NYC.
22 So, thank you, Chair Gutiérrez.

23 CHAIRPERSON GUTIÉRREZ: Thank you.

24 CHRISTOPHER LEON JOHNSON: Happy
25 Holidays. Thank you.

2 CHAIRPERSON GUTIÉRREZ: Thank you, same
3 to you.

4 COMMITTEE COUNSEL: Either one of you
5 can--

6 TOWAKI KOMATSU: Hi, I'm Towaki Komatsu.
7 I'm a Navy veteran. To lead off my testimony,
8 there's a mural on top of the ceiling in the chamber,
9 and I'm going to change the words a bit. A
10 government of the empty seats, by the empty seats,
11 for the people. At the start of this public hearing
12 there were a bunch of City Council members in the
13 room. How many are here now? Mr. Holden, you're
14 good. Ms. Gutiérrez, I just took a note that you
15 were using your cellphone in violation of City
16 Council's rules at 4:32 p.m. while somebody was
17 testifying. So, Mr. Holden used to be a teacher.
18 During tests, they tell students put away your phones
19 and things like that, that can be used for cheating.
20 So with regards to first amendment rights, due
21 process rights, if this is a public hearing, where
22 are the City Council Members to actually hear from
23 the public? Also, DOI Commissioner Strauber was
24 here. I've been DOI repeatedly to make valid
25 complaints against the NYPD. DOI is totally useless.

2 This hearing is also about contracts, NYPD contracts.

3 There was a public hearing yesterday about contracts

4 between HRA and various vendors. The public notice

5 says that you can go to HRA headquarters at 150

6 Greenwich on the 37th floor to see those contracts.

7 Problem is, I've got litigation against HRA. They're

8 still retaliating against me by not letting me in

9 their doors. So, even though it's not relevant to

10 today's public hearing per say, you're the City

11 Council. You have the ability to craft legislation.

12 You have the ability to issue subpoenas. You also

13 have the ability, I guess, to override proposed

14 contracts especially when they're pretty crappy.

15 Sorry for the language. But let me move on. I

16 submitted an exhibit in conjunction with today's

17 testimony. I don't know if maybe Mr. Holden has seen

18 it. This is what I submitted. Basically, I've got

19 ongoing litigation, like I said, against the City.

20 Let me read from some emails in that exhibit. For

21 starters, you currently have Shekar Krishnan, he's a

22 City Council Member. He lives in Jackson Heights. I

23 moved into his former apartment. The NYPD when

24 conducting an illegal surveillance against me also

25 pulled up his name as a former occupant of that same

2 apartment. I previously informed Mr. Krishnan of
3 that. So the point is, if I have no ties with Mr.
4 Krishnan, why in the heck is the NYPD spying on Mr.
5 Krishnan after he used to be a clerk for a federal
6 judge in Brooklyn. So, bottom line is here's an
7 email that was sent by Jacqueline Rothenberg [sp?] on
8 June 28th, 2017 to Howard Redman [sp?] who pled
9 guilty to a felony earlier this year, for obstructing
10 DOI's investigation. Confirmed that he appeared at
11 4WTC on June 6th and served an order to show cause.
12 That OSC and another pending matter were submitted
13 to the court for a decision on June 7th. HRA is
14 still waiting for the written decision. Problem is,
15 I had sealed litigation then. Jessica Ramos
16 illegally had access to that sealed litigation.
17 You're the Committee counsel who I'm looking at right
18 now. So why in the heck are personnel of the City of
19 New York illegally violating New York Supreme Court
20 Judge Barry Ostrager's January 17th, 2017 sealing
21 order, and what is the recourse of when personnel of
22 the NYPD come to your hearings and commit perjury
23 under oath while they're sworn. Thank you.

24 COMMITTEE COUNSEL: Thank you for your
25 testimony. Andrew, you may go ahead.

2 ANDREW: Hello there. My name is Andrew,
3 and I would like to point out that I have nothing
4 against law enforcement. I appreciate the hard work
5 that they do have. Law enforcement has a habit of
6 terrorizing people throughout America. There's a
7 court case that I gave you called Socialist Workers
8 Party versus the Attorney General where law
9 enforcement went around the City making people
10 homeless and getting people fired from their jobs.
11 This is a court case in New York City, and there's an
12 additional flyer that I gave you all that law
13 enforcement-- after people have encounter with law
14 enforcement throughout different states become
15 homeless or fired from their job or can't find a job.
16 So law enforcement is not only terrorizing me-- they
17 go time fired-- but they terrorizing American as
18 well. So that's why I'm here today to ask for an
19 investigation of law enforcement why they keep
20 attacking me. Several times I asked for body cam.
21 They refused to give me body cam. Why is that? Are
22 they trying to hide something? Several times I have
23 encounters with them, and one time where they had
24 brutally assaulted me on 61st Street and Northern
25 Boulevard in Queens. The cameras just magically

2 disappeared off the building. Incredible. Just like
3 Lequan McDonald [sp?] in Chicago when the police had
4 murdered him. They went to Burger King and they had
5 erased the video. It's amazing how law enforcement
6 keep doing the same thing state after state after
7 state. So, I'm asking for an investigation. I'm
8 asking for body came from different incidents that
9 law enforcement had brutally attacked me, not only in
10 New York but Chicago as well. They keep putting me
11 in hospital for some strange reason, and also it's
12 strange how law enforcement when they want to hide
13 evidence, they like to commit people to the psych
14 ward. Two people from NYPD, Nella Gomez [sp?], a
15 Police Detective, had evidence against corruption in
16 law enforcement. What happened? Oh, let's commit
17 her to the psych ward. New York City Police
18 Department, right? Again, this another person who
19 has nothing to do with Nella Gomez, his name is Agent
20 [inaudible], again had corruption, evidence of
21 corruption, of law enforcement, and what happened?
22 They tried to commit him to the psych ward. Oh, this
23 person is crazy. Again, when people have evidence
24 like me, they try to commit me to the psych ward
25 saying that I'm crazy. You can say anything that you

2 want to say, but just take a look at my evidence.
3 The court case is right here in New York City. The
4 court case says law enforcement make people homeless.
5 They get people fired. I have news clips from
6 different states showing that law enforcement make
7 people homeless when they have encounters with them.
8 And Colin Kaepernick is a football-- because I'm
9 pretty sure not everybody watches sports. He's a
10 football player protesting police brutality. What
11 happened? Can't find a job. But he's not
12 [inaudible], but other people are on this list who
13 are not well known as Colin Kaepernick that lost
14 their jobs. Even a veteran came across law
15 enforcement. He too had lost his job. So I'm asking
16 for an investigation and body cam for assistance.

17 CHAIRPERSON GUTIÉRREZ: Thank you. Can I
18 just ask, have you been connected to legal services
19 yet pertaining to that request?

20 ANDREW: I tried several times. Nobody
21 has helped me. They would say that they would help
22 me, and so far, nobody has helped me do anything. I'm
23 still being attacked by law enforcement, and I still
24 have no body cam from New York or Chicago because
25 they want to cover this up.

1 COMMITTEE ON PUBLIC SAFETY WITH COMMITTEE ON TECHNOLOGY 187

2 CHAIRPERSON GUTIÉRREZ: And what borough
3 do you live in?

4 ANDREW: I live in Queens.

5 CHAIRPERSON GUTIÉRREZ: Okay. Let me
6 make note of that.

7 CHAIRPERSON GUTIÉRREZ: You guys have the
8 QR codes?

9 CHAIRPERSON GUTIÉRREZ: I have it, yes.
10 Thank you. Yeah, thank you so much.

11 ANDREW: And what's your name?

12 CHAIRPERSON GUTIÉRREZ: Jennifer
13 Gutiérrez.

14 ANDREW: Okay, like Jennifer Lopez.
15 Okay, thank you.

16 COMMITTEE COUNSEL: If anyone else in the
17 room would like to testify, please come up to the
18 front. Seeing no one else, I'll turn it back to
19 Chair Gutiérrez to close out the hearing.

20 CHAIRPERSON GUTIÉRREZ: Alright, thank
21 you so much to both committee staff and thank you so
22 much to the advocates and everyone who signed up to
23 testify online and here in person, and that adjourns
24 today's hearing.

25 [gavel]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
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 January 12, 2024