# Public Comment: Public Oversight of Surveillance Technology (POST) Act

Eisenberg & Baum, LLP

EB

## DOCUMENT AUTHORS

**Juyoun Han, Esq.:** Juyoun Han is a Partner in Eisenberg & Baum's Artificial Intelligence Fairness and Data Privacy Practice Group. As a litigator, Ms. Han advocates for equity in the use of AI and works to eradicate systemic injustice, stemming from unchecked use of personal data and problematic automated decision systems.

**Patrick K. Lin:** Patrick Lin is a Legal Intern in Eisenberg & Baum's Artificial Intelligence Fairness and Data Privacy Practice Group and a second-year law student at Brooklyn Law School, where he is the vice president of Legal Hackers and a staff member of the Brooklyn Law Review. Prior to law school, Patrick worked on data governance and regulatory compliance as a technology consultant.

*(*Thanks to Rebekah Tweed for contributions in organizing the Forums)*

## CONTRIBUTORS & COMMENTERS

**Ke Yang, NYU Tandon School of Engineering**
**Albert Fox Cahn, S.T.O.P.**
**Brandon del Pozo, Brown Univ.**
**Reyna Lubin, Eisenberg & Baum, LLP**
**Renee Cummings, Urban AI**
**Phillip Hamilton, Hamilton Clarke, LLP**
**Laura Hecht-Felella, Brennan Center for Justice**
**David C. Benjamin, Adept Corporation Limited**
**and approximately 85 concerned members of the public**

## TABLE OF CONTENTS

**NYPD USE OF SURVEILLANCE TECHNOLOGY**
**POST ACT – PUBLIC COMMENT**
*Compiled and Drafted by Eisenberg & Baum, LLP*
*on behalf of members of the public who participated in public forums hosted on*
*February 10 & 17, 2021*

**"IN A DEMOCRACY, THE ACCOUNTABLE AGENTS OF THE PEOPLE OWE THE PEOPLE AN ACCOUNT OF WHAT THEY HAVE BEEN DOING, AND A REFUSAL TO PROVIDE THIS IS SIMPLE INSOLENCE." - JEREMY WALDRON**

## ABOUT THE POST ACT

On June 18, 2020, when the New York City Council voted 44-6 to enact the Public Oversight of Surveillance Technology (POST) Act (Int 0487-2018), members of the public ("we" hereinafter) fully expected increased transparency and oversight of the New York Police Department's use of surveillance technologies and information sharing networks. On January 11, 2021, draft surveillance technology impact and use policies ("Draft Policies") were posted on the NYPD website. Members of the public were invited to review the Draft Policies and provide feedback until February 25, 2021.

On February 10th & 17th, 2021, the law firm of Eisenberg & Baum, LLP's AI Fairness and Data Privacy Department organized and hosted two public forums, attended by approximately 90 members of the community to share knowledge, inspire civic discussion, and gather public comments. To lead forum discussions, Eisenberg & Baum, LLP invited panel speakers with a broad range of experiences and fields of expertise. The forums were designed to create a space for individuals with varied backgrounds to freely share their thoughts. This submission compiles comments expressed by the forum participants throughout the public forums and in writing.

## PRELIMINARY COMMENTS: PROCEDURAL DEFICIENCIES IN NYPD'S DRAFT POLICIES

Public commenting is a futile exercise unless the public is sufficiently informed about the subject matter upon which it is asked to provide comments. The Draft Policies disclosed on January 11, 2021 contained numerous serious deficiencies that would render a public commenting process ineffective. Pertinently, the Draft Policies: (1) include little to no substantive information or explanation about how the systems work in concert with one another; (2) contain no information about the number and location of surveillance technology devices even though such information is critical to assessing their implications upon individual privacy and equity; (3) demonstrate little to no effort to communicate the technological functions and information in a way that is aptly understood by a non-technical audience; (4) provide no information related to datasets or software models used, and fail to name the commercial vendors it purchases the software from and maintains operations with which makes a substantive review impractical; and (5) contain inaccurate and vague boilerplate language that essentially asks members of the public to take their words at face value.

We are concerned that these deficiencies would reduce the public commenting process to a hollow gesture. Following the examples of other cities that have previously enacted ordinances

similar to the POST Act, the NYPD should (1) name the authors, affiliations, and departments responsible for drafting the policies that were disclosed; (2) hold several public hearings with independent interdisciplinary auditors to explain the day-to-day use of the technology and its impact on civilian's lives, answer questions from the public, and provide informational materials to the public; (3) make available information about the datasets, algorithmic model specifications, vendors and developers, and funding for each of the technologies; and (4) extend the public commenting period until the public has been sufficiently informed about the technologies and has the opportunity to comment on each of the Draft Policies. Numerous better practices can be found outside of NYC and the United States including, but not limited to, Seattle, Oakland, and San Francisco.

Despite these obvious deficiencies in the disclosed Draft Policies, members of the public have made their best efforts to provide input in areas of concern during the public forums hosted by Eisenberg & Baum, LLP.

## PUBLIC FORUM: WHAT DO WE THINK ABOUT NYPD'S USE OF SURVEILLANCE TECHNOLOGY?

In order to inform ourselves about the capabilities of NYPD's surveillance technology and discuss the concerns that arise with the ubiquity of this technology, Eisenberg & Baum, LLP's AI Fairness and Data Privacy Department organized and hosted two public forums to share knowledge, inspire civic discussion, and gather public comments. To lead forum discussions, Eisenberg & Baum, LLP invited panel speakers with a broad range of experiences and opinions including prosecutors and defense attorneys to activists and former NYPD officers. The forums were designed to create a space for individuals with varied backgrounds to share their thoughts. The forums were free for anyone to attend and participate.

### COMMENTS & NOTES FROM THE FIRST FORUM (FEB. 10, 2021)

In the first forum, held virtually on February 10, 2021, approximately 60 members from a cross-section of the community both within and outside of NYC joined. The discussions were led by the following Panel Speakers, moderated by **Juyoun Han, Esq.**:

- **Renée Cummings**: Renée Cummings is a criminologist and AI Ethicist. She is the first Data Activist in residence at the University of Virginia, joining the School of Data Science in the fall of 2020. Cummings is a Community Scholar in AI & Criminal Justice at Columbia University, as well as the founder of Urban AI, a Certified Ethical Emerging Tech Examination Developer for CertNexus, and a Founding board member of Springer's AI and Ethics Journal.

- **Albert Fox Cahn**: Albert Fox Cahn is the Surveillance Technology Oversight Project's ( S.T.O.P.'s) founder and executive director, a fellow at the Engelberg Center on Innovation Law & Policy at N.Y.U. School of Law, a member of the NYU Alliance for Public Interest Technology, and a columnist for Gotham Gazette. As a lawyer, technologist, writer, and interfaith activist, Mr. Cahn began S.T.O.P. in the belief that emerging surveillance technologies pose an unprecedented threat to civil rights and the promise of a free society.

- **Ke Yang**: Ke Yang is a PhD candidate in Computer Science at the Tandon School of Engineering at New York University and a member of the Visualization and Data Analytics Research Center whose current project examines the impact of technical bias on the model serving in data science pipelines. Yang's research interests include ethical topics such as fairness, accountability, transparency, interpretability, and the social impact of the algorithms in data science pipelines.

- **Reyna Lubin, Esq**.: Reyna Lubin is an associate in the Eisenberg & Baum Law Center for Deaf and Hard of Hearing. Prior to joining the firm, Ms. Lubin was an Assistant District Attorney at the Kings County District Attorney's Office. At the DAs office, Ms. Lubin dedicated herself to helping victims of domestic violence. Ms. Lubin is a regular speaker on issues relating to domestic violence, police brutality, and racial injustice.

- **Phillip C. Hamilton, Esq**.: Phillip C. Hamilton is an experienced trial attorney and litigator in the areas of complex state and federal criminal defense, civil rights actions, and contractual formation and disputes. Since 2015, Phillip has primarily defended white-collar professionals charged with serious, high-profile offenses. Phillip is also an Adjunct Professor of Law at the Benjamin N. Cardozo School of Law, and regularly guest lectures trial advocacy and negotiation seminars in law schools around the New York City metropolitan area.

During a 75-minute discussion, the following comments and concerns were raised by the participants, which are organized by theme and summarized below (*Note: The public comments are collected and compiles, and the comments may not align with each and every participant's or panel speaker's individual opinions and/or perspectives):

1. **Accountability**
   - NYPD should establish an accountability framework that allows for public oversight and democratic accountability.
   - NYPD should establish a mechanism enabling taxpayers' oversight over detailed funding apportioned for the purchase, maintenance, upgrading, and testing of surveillance technology used in the City.
   - NYPD should establish a mechanism enabling taxpayers' oversight over vendors' and subcontractors' use of individuals' data.
   - NYPD should disclose all the ways that the individuals' data collected may be used, and whether there are any profitable gains from the collection, usage, and sale of the individuals' data.
   - Following the model of Oakland Privacy Commission, there should be an independent board composed of residents, law enforcement, and community activists who have approval authority over the surveillance technology being used.
   - On the human side of the use of this technology, are there ethical guidelines or "checks and balances" that can lessen the risk of bias to acceptable levels?

2. **Transparency**
    - NYPD should regularly submit its surveillance technology to independent, third-party monitors and the result should be made public.
    - The comprehensive audit should include technological (data sets, models, implementation), socio-economic, financial, internal training and policy implementation procedures within the NYPD, and audit of all vendors and sub-vendors who develop and update the technology.
    - NYPD should disclose the surveillance technologies that were considered and evaluated for use in the City, and disclose the criteria and standards by which the Department chose the tech products/vendors.
    - NYPD should also disclose whether the criteria for selecting and evaluating the tech products/vendors included racial bias detection.
    - AI can nurture political freedom and democracy when people have access to and control over the data constituting and representing their identity.
    - Transparency is an important value, as is privacy. But neither are absolute, and the critical task is to determine limits of both.
    - Transparency and accountability create public confidence and it's very low. One thing that we are seeing with the technology is that ability to alter or manipulate the confidence threshold.
    - Generally, it appears that all of these technologies have benefits and drawbacks, but there needs to be more transparency first, and then, more safeguards on how these technologies and the data they collect will be used.

3. **Public Education, Right-to-Know, and Training**
    - NYPD should prioritize public education for all members regarding the use of surveillance technology.
    - In addition to the disclosure of Draft Policies, NYPD should hold regular public hearings that explain the technological elements and functions as well as its implications to non-tech audience.
    - NYPD should disclose statistics and locations where certain technologies are deployed (CCTVs, facial recognition, etc.).
    - FOIL requests seeking access to information about the use, impact, and deployment of surveillance technology should be expedited and maximize the information given to the public, and NYPD should not issue rote-denials on baseless rationales such as revealing investigative techniques, inter- / intra- agency materials, and more.
    - In areas where surveillance technologies are concentrated, members of the local community should be informed and representatives of those districts should have input on mitigating any concerns related to bias.
    - Training manuals and mandatory training sessions that the use, ethics, and social impact surrounding surveillance technology should be required of all members of law enforcement, criminal lawyers (prosecution and defense) and members of the judiciary.

4. **Technology, Data Sets, Accuracy**
    - NYPD should disclose the accuracy threshold of the surveillance technology used

- NYPD should disclose the data sets, inputs and outputs of the technology and AI models they are using so that their accuracy and transparency can be tested.
- NYPD with public stakeholders should focus on developing an "accuracy threshold" and eradicate and/or pause the use of any technology that demonstrates biased inaccuracies in certain populations especially along racial, gender lines.
- The use of facial recognition should be altogether banned and/or paused.
- Most of these technologies raise multiple issues, and resolving some may not resolve others. But if, for example, some can be improved, will that constitute an argument for moving ahead with them – e.g., more accurate facial recognition technology, the expansion of surveillance from street crime and so counteracting some of the racial bias currently seen? How many of the problems are "technical" and how many are inherent to surveillance of any kind?
- AI can nurture political freedom and democracy when people have access to and control over the data constituting and representing their identity.
- All AI is predictive; that is where it has the chance for misidentification. Is the ask of NYPD now only to say what technology they are using and how? Should it not be about the transparency of the accuracy and recall rate (i.e. how often does it say "Yes" and what percentage of time the AI is correct when it says "Yes").
- Lots of great concerns have been brought up here about these technologies, which all seem like they have pros and cons, some weighing one way more than the other. Is there an accepted or suggested "accuracy threshold" to force only technologies that are "good enough" to be used by law enforcement?
- If you check for some segment of the population, like Black residents or women, the accuracy might be low based on bias in the data used to train the AI and that is not typically checked.
- Even though the average performance is OK, they certainly are not OK for some communities or for some groups due to the issues in the data or due to the issues in the development of the tools or the usage of the tools.

**5. Criminal Justice**

- NYPD, the Prosecutors' office, Defense attorneys' bar, and judiciary should set forth rules limiting the use of surveillance technology to certain kinds of crimes, investigations, and release those rules to the public.
- Any use of surveillance technology involved in a criminal case should be disclosed to the criminal defendant and counsel as well as the prosecution.
- Every person should be able to see his or her data portfolio in the NYPD's collection of data and have the right to delete inaccurate or expunge appropriate information.
- At any given moment, you could be dragged into a criminal prosecution just based on misidentification or because on the fact that your data is part of a sweep and it's being done without a warrant.
- How do we deal with over-policing certain Black and Brown communities with more technologies?
- What's really concerning to me about facial recognition is that we don't know what's going on. I have no idea who initiated this use of facial recognition. It wasn't me; it wasn't the prosecutor's office; it might be the NYPD, and who is checking if that's even

legal or not. I like the use of my technology because it's gone through a system of checks and balances to determine if this is appropriate, to determine if it is reasonable to use.

- In terms of the civil rights of my client, more often than not, I have a lot of concerns . . . because to the extent that you are approaching suppression litigation, the question that the court is always going to start with is "Was there a reasonable expectation of privacy?"
- The technology is so new and because the law is still behind the technology and law enforcement has this tool in their hands, the tool can turn into a toy and many times it moves from you just using this technology or experimenting with this technology and where without reasonable suspicion, you become a person of interest.
- My fear as we talk about slippery slopes and just kind of moving forward is because we are living in such a surveilled state because every where we go all of this is being collected and from the minute I step outside of my father's house, there is a camera on the main street. Where can I go at this point that I won't be surveilled?
- To what extent is the "digital stop-and-frisk" appropriate, or perhaps it is simply not appropriate at all? Studies of some of the surveillance technologies themselves, such as facial recognition, have been shown to be ineffective at identifying Black faces, for instance. While the use of surveillance technology might be posed as a neutral alternative to biased police practices, it is highly questionable as to whether we are actually "safer" with police surveillance technology in communities of color.

## COMMENTS & NOTES FROM THE SECOND FORUM (FEB. 17, 2021)

In the second forum, held virtually on February 17, 2021, approximately 25 members from a cross-section of the community both within and outside of NYC joined. The discussions were led by panel speakers and moderated by **Juyoun Han, Esq.**:

- **Laura Hecht-Felella, Esq.**: Laura Hecht-Felella is the George A. Katz Fellow with the Brennan Center for Justice's Liberty and National Security Program. She focuses on issues related to civil rights and technology as well as content moderation and online speech, and has been actively involved in the Brennan Center's policing and technology work.

- **Brandon del Pozo**: Brandon del Pozo, PhD served 19 years in the NYPD and four as the chief of police of Burlington, Vermont and is now a postdoctoral researcher at Brown University, and believes improving the quality of American policing lies in using the goals, methods and metrics of public health to shape and guide its responses to both crime and non-criminal risk behaviors. He's been featured in the New York Times and appeared on the MSNBC podcast "Why Is This Happening?" with Chris Hayes.

During a 60-minute discussion, the following comments and concerns were raised by the participants, which are organized by theme and summarized below (*Note: The public comments are collected and compiles, and the comments may not align with each and every participant's or panel speaker's individual opinions and/or perspectives):

1. **Third-Party Audits on Technology Functions and Use**
    - There should be transparency in providing more information to the public about the surveillance technology used. There is also huge value in audits that are made public.
    - The contents of audits should be critically looked into, so as to ensure that there are proper oversight mechanisms in place.
    - Self auditing is not ideal in terms of accountability because of the danger of "end[ing] up with boilerplate responses that don't actually provide much information but are kind of a bureaucratic check, which actually can maybe do more harm than good so I think that audits are can be really valuable especially when they're done by a third party."
    - Third-party audits that focus on how the technology is actually used versus how it is being presented to the public are valuable. For example, the Policing Project at the NYU School of Law audited Baltimore's Aerial Investigation Research (AIR) Program.[1] While the NYU audit acknowledged that the legal implications are somewhat speculative in part because the U.S. Supreme Court rulings do not adequately cover such technology, the audit did hone in on two specific concerns. First, Baltimore's Board of Estimates voted to approve the project, not the City Council. Because the program collects data on Baltimore residents on a daily basis, it is imperative that approval comes from the city's entire elective body, and not a smaller board. Second, Baltimore police relied on "supplemental reports" to justify following the suspects beyond the point of the initial crime, and for multiple days. The initial agreement did not approve Baltimore police to track suspects long after the initial crime. The Policing Project at NYU published its audit findings in November 2020.[2]
    - Audit should go beyond just the technology itself, but address the effectiveness, use, and impact of the technology. The National Institute of Standards and Technology (NIST), for example, tests various facial recognition vendors for their accuracy with different demographics.[3] In a report published in December 2019, NIST found that when looking at instances in which an algorithm wrongly identified two different people as the same person, algorithms had the highest error rates for Native Americans as well as high rates for Asian and Black women, particularly in facial recognition systems that relied on mugshot databases.
    - Where there is tangible evidence that the technology is flawed (such as facial recognition), it should not be used until it can be audited and vetted as it can have deleterious consequences to individual rights.
    - Presumably one of the advantages of an audit -- along with its conclusions -- is that it may help drive the technology forward, so that it works better. That has definitely been the case with drone technology, and I imagine might well be very helpful in the cases of facial recognition and CCTV technology.

---

[1] P. Jackson, *Baltimore's surveillance plane potentially infringes on rights, audit finds, even though police mostly followed the rules*, BALTIMORE SUN (Dec. 12, 2020), https://www.baltimoresun.com/news/crime/bs-md-ci-cr-aerial-program-review-spy-plane-20201212-a5cnfitg75dexdsjgzcciqdhye-story.html.

[2] Civil Rights and Civil Liberties Audit of Baltimore's Aerial Investigation Research (AIR) Program, THE POLICING PROJECT AT NYU LAW (Nov. 2020), https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5fc290577acac6192a142d61/1606586458141/AIR+Program+Audit+Report+vFINAL+%28reduced%29.pdf.

[3] Grother et al., *Face Recognition Vendor Test NISTIR 8280*, NAT'L INST. OF STANDARDS AND TECHNOLOGY (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

2. **Safeguards and Civil Society Oversight**
    - Gleaning from Community Control Over Police Surveillance (CCOPS) Models[4] of other cities (e.g. Oakland), below are some safeguards and oversight mechanisms.
        - A city council (body of elected officials) or a similar body composed of residents and experts who can approve or veto the use of technology.
        - Prohibiting the use of Non-Disclosure Agreements between the NYPD and vendors who develop the software. The police department should not be bound by NDAs that prevent release of information about the software to members of the public.
        - Granting a private right of action that allows individual civilians to take action to hold the police accountable for abuse of surveillance technology that encroaches on civil rights.

3. **Establishing a "Serious Crime" Threshold for Surveillance Technology**
    - I think we should give serious thought to surveillance technologies that allow us to bring surveillance power to very minor violations of the law.
    - Certain surveillance technology (that can be vetted based on concrete review of its accuracy and fairness) may be legitimately used for tracking suspects who are committing serious crimes to better focus NYPD efforts, but the worry is that once technology is used, it becomes a justification to expand its use in invasive and disproportionate ways. Hence, there should be clear, transparent and auditable policies about what the technology will be used for, and when it won't be used, along with an audit about whether the technology is accurate and equitable to be used at all.
    - If the NYPD came to lift fingerprints at the scene of every crime, it would be excessive and invasive – similarly, we should not be using technology for minor infractions which gives the government the capacity to invade into our private spheres in life.

4. **Financial Transparency between Tech Companies and NYPD**
    - The biggest threat to privacy is Corporate America.
    - Facial recognition technologies and many surveillance technologies that are already in use have corporate ties (i.e., social media on the internet and other private spaces). There is a monetization incentive to offer such invasive technology, especially facial recognition, to police department. Profit driven use of surveillance technology is at odds with civil rights and these incentives need to be realigned.
    - NDAs should not be used. The research and development of the technology should be revealed to the scientific community and the public for review after a certain time period, akin to how the NIH and medical science community discloses their research and data to the science community after a period of time. The protected interest in surveillance technology should be the public good, and not the financial interest of tech companies.

5. **Data Use and Storage Oversight**
    - Should we shift our focus from looking at here at 36 technologies to how the technologies collect data and how that data is monetized by use of these technologies?

[4] Degroff & Cahn, *New CCOPS On The Beat*, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT (Feb. 10, 2021), https://www.stopspying.org/ccops.

- When we hear about how technology has targeted people of a certain profile, and it was because of the data, then we know data seems to be the culprit. So should we shift our focus to data and control the, the laws around data mining and usage. Technologies can change forms, but the problems with the underlying data would still remain.
- My area of research is on value creation from data. Even if NYPD's policies say that they delete data after a certain amount of time, the learning from the data is already gone into the brains of the AI, so the machine could look for that pattern the next time they see the data, and even though the old data is deleted, it forms the learning process which allows software firms to monetize previous data.
- How the data is used is as at least as important as how much of it is collected and where it's stored and what for. What types of data you're collecting reveals a tremendous amount about your thinking and your intentions and in America it's bound to be racialized and follow along the lines of class. So I think we need to properly regulate the storage of data and think about how its application can be fair.
- NYPD should disclose more about how the data is secured and stored, and how a particular set of data is categorized as criminal justice data.
- NYPD must establish an easy way for an average person to find out whether the NYPD's data stored about them is accurate.
- Do the 36 surveillance tech companies share data with each other, and/or do they share the same cloud storage? If so, provide details to the public on cross sharing of information and provide transparency on cloud storage services as some use the data for their own AI training.
- What cloud storage is the NYPD using for each technology? What does the cloud storage NDA look like?
- "I don't want the NYPD to store my data. This violates my privacy rights. How secure is the data that NYPD collects on citizens?"

**6. Need for Comprehensive Oversight**

- I think a lot of times when people are talking about surveillance technologies, they talk about them in isolation for example, there's facial recognition bans or oversight intended to talk about stingrays which is another technology, but it is the layering of the technologies and the accumulation of data, and in the long run, that can be so problematic.
- NYPD should explore a comprehensive approach to enhancing oversight "through the utilization of an accountability assessment tool that allows an organization to take stock of its surveillance operations, and through the creation of multi-disciplinary Techno-ethics Boards that could be worked into the process of building and applying surveillance programs."[5]

[5] Kleinig, J. et al, *Security and Privacy: Global Standards for Ethical Identity Management in Contemporary Liberal Democratic States*, p. 228, ANU PRESS (2011 ed.), Digital version available at: https://press-files.anu.edu.au/downloads/press/p162481/pdf/book.pdf. (Recommended in entirety, special focus on chapters VII. Surveillance Technologies and Economies, and IX. The Complexities of Oversight and Accountability).

7. **Need for NYPD to Gain Public Trust**
    - There is a general mistrust toward the NYPD that is further compounded by mistrust towards the use of technology in policing. But there are crimes that can be prevented if the police worked in better concert with the public and they have not. Police more often resort to using technology to solve crimes because they are unable to gain public cooperation in investigations, which then feeds into more distrust by the public creating a vicious cycle. The solution is community cooperation and community participation.

8. **Legal Responsibility and Private Right of Action**
    - Technology companies and NYPD should be subject to a private right of action so that harmed individuals have legal recourse.
    - The names of vendors, software firms, and contractors, as well as their roles in developing and deploying the surveillance technology, should be disclosed.

## ADDITIONAL INFORMATION ABOUT NYPD SURVEILLANCE TECHNOLOGY THAT SHOULD BE DISCLOSED

There are numerous inaccuracies and vague descriptions in the Draft Policies regarding the impact and use of each of the 36 technologies posted on January 11, 2021. While a few examples are addressed and questioned in this section, the NYPD should provide additional information regarding all 36 technologies.

1. **Cell-Site Simulators (Stingrays)**
    - Cell-site simulators can locate and track individuals moving throughout public and private spaces within their radius. The NYPD should publicly disclose the number of cell-site simulators deployed in each zip code.
    - From May 2020 to September 2020, in how many instances has the NYPD used cell-site simulators in connection with any investigations surrounding the Black Lives Matter protests?[6]
    - Draft Policies state that the cell-site data is not retained by the NYPD, but will the vendors retain the data? How does the NYPD control the vendors' data usage and retention practices?

2. **Criminal Group Database (Gang Database)**
    - How does the NYPD validate the authenticity and validity of "self-admission" with respect to criminal group membership, especially as it relates to "social media posts admitting to membership in a criminal group"?
    - What safeguards are in place to prevent police misinterpretation of admissions or social media posts?
    - What safeguards are in place to prevent non-gang related civilians living in "gang areas" from being over-surveilled and stripped of their privacy rights?

[6] K. Zetter, *How Cops can Secretly Track your Phone*, THE INTERCEPT (July 31, 2020), at https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/

- NYPD should disclose statistics on how many people are removed from the database upon review every three years and the reasons for removal.
- NYPD should disclose statistics on the error rates in which people who are not affiliated with gangs had been placed in the gang database.
- NYPD should reveal the proportion of Black and Latinx individuals in the gang database compared to the rest of the population.
- NYPD should enable civilians to gain information on whether they are in the database, and how someone can challenge or appeal their inclusion in the database.[7]
- NYPD should compare its database to gang databases in cities that were found to be abused, inaccurate, and/or racially biased, such as Chicago and Portland, and justify the existence of the NYC gang database.[8]

**3. Facial Recognition**

- How does NYPD's facial recognition technology "not use artificial intelligence, machine learning, or any additional biometric measuring technologies"? Without AI, how are the images compared with the collected images?
- Are images extracted from police body cameras used in the facial recognition database?
- How does NYPD justify the use of facial recognition technology when numerous reports prove that the technology is prone to lead to misidentification, inaccuracies, and racial/gender bias?[9]
- Are images of minors added to the facial recognition database or used in finding matches, and if so, how frequently?[10]
- How are these images stored, secured, and how can one find out if their face images are in the NYPD's facial recognition database or the database of NYPD's vendors?
- Which vendors do NYPD use for facial recognition and how much taxpayer money is spent on purchasing facial recognition related products or services from these vendors?
- Given that NYPD's facial recognition is used without any court authorization, when and how is the use of facial recognition revealed to criminal defendants who are arrested? When and how is the use of facial recognition revealed to criminal defense lawyers?

---

[7] Y. Khan, *Damning Report on NYPD Gang Database Increases Calls to End 'A Tool of Mass Criminalization*,' GOTHAMIST (Dec. 13, 2019), https://gothamist.com/news/damning-report-nypd-gang-database-increases-calls-end-tool-mass-criminalization.

[8] Trujillo & Vitale, *Gang Takedowns in the De Blasio Era: The Dangers of 'Precision Policing'*, BROOKLYN COLLEGE POLICING SOCIAL JUSTICE PROJECT (2019), https://static1.squarespace.com/static/5de981188ae1bf14a94410f5/t/5df14904887d561d6cc9455e/1576093963895/2019+New+York+City+Gang+Policing+Report+-+FINAL%29.pdf.

[9] Clare Garvie, *Garbage In, Garbage Out*, GEORGETOWN LAW CENTER ON PRIVACY & TECHNOLOGY, https://www.flawedfacedata.com/.

[10] Goldstein & Watkins, *She was Arrested at 14. Then Her Photo Went to a Facial Recognition Database*, NEW YORK TIMES (Aug. 1, 2019), https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html.

4. **ShotSpotter**
   - How does NYPD's ShotSpotter technology "not use artificial intelligence, machine learning, or any additional biometric measuring technologies?"
   - What is the false-positive rate of ShotSpotter in the time that it has been used in NYC?[11]
   - How many arrests and convictions have resulted from ShotSpotter use?
   - What is the basis for the statement that ShotSpotter devices "cannot be used to covertly listen to conversations, street-noise, or any non-gunfire acoustic data" where it has been proven to pick up street noises and utilized to target fireworks?

5. **Social Network Analysis Tools**
   - What triggers the monitoring of a specific social media account, and by what standards?
   - NYPD should disclose the statistics regarding race and gender of all social media accounts that have been subject to monitoring by social network analysis.
   - Which vendors do the NYPD rely on to develop the social network analysis tool?
   - When and under which standards are undercover NYPD officers authorized to send connection or friend requests to certain social media accounts for monitoring purposes?
   - Can a member of the public request to see the personal social network data that the NYPD retains about him- orherself?
   - What types of datasets are used to train social network analysis tools to detect and alert investigators of social media activities?
   - Are social network analysis tools used to narrow down an investigation based on locations or keywords? If so, what safeguards are in place to prevent violation of free speech rights and discriminatory impact based on the use of this technology?

6. **Data Analysis Tools**
   - What type of data is collected to train artificial intelligence, and have those datasets been scrutinized for disparate impact?[12]
   - What kind of attributes, words, terms, and proxies are used to process the data in the data analysis tool?
   - Which vendors are used to develop the NYPD's data analysis tools?
   - What are the annual costs associated with the purchase and maintenance of data analysis tools?

7. **Domain Awareness System (DAS)**
   - What has justified the NYPD's use of more than $31.4 million in developing the DAS which is described as the "largest capital outlay for Fiscal 2020?"[13]

---

[11] P. Shakur, *Gunshot Detection Technology Raises Concerns of Bias and Inaccuracy*, CODA (Mar. 3, 2020), https://www.codastory.com/authoritarian-tech/gun-violence-police-shotspotter/.
[12] M. Griffard, *A Bias-Free Predictive Policing Tool?: An Evaluation of the NYPD's Patternizr*, 47 FORDHAM URB. L.J. 43 (2019), https://ir.lawnet.fordham.edu/ulj/vol47/iss1/2.

[13] Report to the Committee on Finance and the Committee on Public Safety on the Fiscal 2021 Executive Budget for the NYPD, NEW YORK CITY COUNCIL (May 14, 2020), https://council.nyc.gov/budget/wp-content/uploads/sites/54/2020/05/FY21-NYPD-Executive-Report-1.pdf.

- DAS comprises more than 20,000 CCTV cameras, police-worn body cameras, license plate readers, radiation scanners, drones, 911 calls, and unknown commercial and interagency intelligence databases, and has real-time tracking capabilities – what oversight is in place for such a mass surveillance system?
- How long is information stored on DAS, and what mechanism is available for civilians to check what personal information is stored on or associated with DAS?
- How was DAS used by the NYPD in surveilling the Black Lives Matter protests?[14]

[14] M. Morales & Ly, *Released NYPD emails show extensive surveillance of Black Lives Matter protesters*, CNN (Jan. 18, 2019), https://www.cnn.com/2019/01/18/us/nypd-black-lives-matter-surveillance/index.html.