Brooklyn Defenders

Brooklyn Defender Services
177 Livingston St, 7th Fl
Brooklyn, NY 11201

Tel (718) 254-0700
Fax (718) 254-0897
info@bds.org

TESTIMONY OF

Elizabeth Daniel Vasquez,
Director, Science and Surveillance Project

BROOKLYN DEFENDER SERVICES

Presented before

The New York City Council Committees on Public Safety and Investigation and Oversight

Oversight Hearing on DOI's Office of the Inspector General for the NYPD.

April 11, 2022

My name is Elizabeth Daniel Vasquez. I am the Director of the Science & Surveillance Project at Brooklyn Defender Services (BDS). BDS is a public defense office whose mission is to provide outstanding representation and advocacy free of cost to people facing loss of freedom, family separation and other serious legal harms by the government. I thank Chairs Hanks and Brewer for inviting us to testify today about the DOI's Office of the Inspector General for the NYPD.

For over 25 years, BDS has worked, in and out of court, to protect and uphold the rights of individuals and to change laws and systems that perpetuate injustice and inequality. We represent approximately 25,000 people each year who are accused of a crime, facing loss of liberty, their home, their children, or deportation. Our staff consists of specialized attorneys, social workers, investigators, paralegals and administrative staff who are experts in their individual fields. BDS also provides a wide range of additional services for our clients, including civil legal advocacy, assistance with educational needs of our clients or their children, housing and benefits advocacy, as well as immigration advice and representation.

Many of the people that we serve live in heavily policed and highly surveilled communities. These communities bear the brunt of the NYPD's privacy-destroying and abusive behavior, including through the wrongful seizure of their personal belongings, the unannounced addition of their deeply personal information (including DNA profiles, social networks, and every day habits) into unregulated law enforcement databases like the gang database, and the unceasing subjection of "the privacies of life"[1] to police gaze through cameras, sensors, microphones, digital scraping tools, and their underlying, mass-aggregating databases like the Domain Awareness System.

[1] *Carpenter v. United States*, 138 S. Ct. 2206, 2213–14 (2018) ("Although no single rubric definitively resolves which expectations of privacy are entitled to protection, the analysis is informed by historical understandings of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted. On this score, our cases have recognized some basic guideposts. First, that the Amendment seeks to secure the privacies of life against

Brooklyn Defenders

I want to thank the Committees on Public Safety and Investigation and Oversight for holding an important discussion not only on the functioning of the DOI's Office of Inspector General for the NYPD, but also more broadly and critically on the kind and quality of public oversight required to police the most technically-advanced law enforcement agency in the world.

The Urgent Need for Surveillance Oversight

Twenty years after 9/11, a combination of security choices and technological advances (including increased processing speeds and decreased storage costs) have put our society on track to become a true surveillance state. Reliance on big data techniques is in vogue across all sectors. And since late 1960s federal investment in the "professionalization" of policing elevated technology as the way forward in the criminal legal sector, law enforcement has wholeheartedly embraced surveillance technology as the future of policing.

Nowhere are these realities more true than in post-9/11 New York City.[2] We have outlined in prior testimony to the Public Safety Committee the breadth of technologies owned and deployed by the NYPD.[3] Today, however, we focus instead on the lack of oversight, regulation, and constraint in this space. As a society, we are at an inflection point; the decisions we make now will determine whether a free society remains possible or whether we lose that vision forever.

As Professor Andrew Ferguson noted before the United States Congress in 2019, "the Fourth Amendment will not save us from the privacy threat posed by [surveillance] technolog[ies]. The Supreme Court is making solid strides in trying to update Fourth Amendment principles in the face of new technology, but they are chasing an accelerating train and will not catch up. Legislation is needed to respond to the real-time threats of real-time technology."[4]

The Role of the DOI's Office of Inspector General for the NYPD

Launched in 2014, the Office of Inspector General for the NYPD was tasked by the City Council with "the goal of enhancing the effectiveness of the department, increasing public safety, protecting civil liberties and civil rights, and increasing the public's confidence in the police force, thus building stronger police-community relations."[5]

Since its inception, the OIG-NYPD has issued a total of 17 reports. Only two of those reports have addressed the impact of NYPD's bloated surveillance apparatus on civil liberties and civil rights or the public's confidence in the police force. This is a grave mistake.

---

arbitrary power. Second, and relatedly, that a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance."

[2] Ali Watkins, "How the NYPD is Using Post-9/11 Tools on Everyday New Yorkers," NYTimes (Sept. 8, 2021).

[3] *See* https://bds.org/assets/files/City-Council-Mayors-Blueprint-Joint-Defender-Testimony-FINAL.pdf

[4] Andrew Guthrie Ferguson, "Written Testimony of Professor Andrew Guthrie Ferguson before the House of Representatives Committee on Oversight and Reform," Hearing on Facial Recognition Technology: Its Impact on our Civil Rights and Liberties (May 22, 2019).

[5] Local Law No. 70 § 1.

As a civilian body vested with broad investigatory powers, it is the role of the OIG-NYPD to explore systemic issues within the NYPD that perpetuate biased policing, have a disproportionate impact on Black, brown, and low-income communities, and escape other structures of oversight and accountability. Despite this set of duties, the OIG-NYPD has presided over an era of expanded and expanding police technological armament without conducting any investigations into that growth.

POST Act Responsibilities

The Public Oversight of Surveillance Technology (POST) Act of 2020 was passed by the City Council to increase transparency around the NYPD's growing surveillance arsenal. The POST Act required the NYPD to publicly publish impact and use policies for each surveillance technology the Department owned. Those policies were required to address not only capabilities and implementation, but also information about the disparate impact of the technologies' use.

In ostensible compliance with the POST Act, the first set of draft disclosures from the Department were published on January 11, 2021. Following a 45-day comment period, the Department then issued final disclosures on April 11, 2021. During the public comment period, multiple commenters and entities noted that the NYPD's disclosures were inaccurate, were essentially copy-and-paste jobs, and fundamentally failed to comply with the POST Act's requirements.[6] Many of these public comments were sent directly to the Department of Investigation, in addition to the NYPD.

Even without these public comments and filed grievances about the NYPD's failure to comply with the law, the POST Act itself requires the OIG-NYPD to prepare an annual audit of the NYPD's POST Act disclosures, assessing compliance, describing known or suspected violations, and publishing recommendations. It has been a full calendar year since the NYPD first issued their final disclosures and the OIG-NYPD has not publicly reached out to commenters who raised concerns about the NYPD's POST Act compliance *or* published the legally required annual audit of the Department's disclosures.

The NYPD's POST Act disclosures did uncover a stark fact related to the need for surveillance oversight specifically. Review of those disclosures as a body reveals that the Department does not believe a warrant is required before using over 85% of the technologies they identify. Whether the NYPD is correct about the lack of constitutional or statutory constraint in this space or the Department's ability to operate these technologies without seeking court oversight aside, this departmental perspective merely highlights the critical need for legislative and civilian oversight body intervention in this space.

Broader Oversight Responsibilities for Surveillance and Science

[6] *See, e.g.,* Public Comments submitted by Brooklyn Defender Services; a Coalition of Advocates and Academics; the New York Civil Liberties Union; the Electronic Privacy Information Center; and the Legal Aid Society.

Even without direct legislative direction to investigate the NYPD's use of science and surveillance technology, it is clear that the OIG-NYPD has and *should have* broader obligations of oversight and investigation in this space than the Office is currently acknowledging. The abysmal pace of the Office's investigations and the startling lack of creativity in identifying, opening, and pursuing investigations calls into question the effectiveness of the DOI's OIG-NYPD itself.

Areas for necessary oversight by the OIG-NYPD include:

1. **Criminal Group Database**

The NYPD maintains a secretive, internal list called the Criminal Group Database—also known as the Gang Database—in which the Department labels almost exclusively young Black and Latinx New Yorkers as gang members. Over 99 percent of the people on the database are non-white. There is no independent oversight of who is placed in this database, individuals do not need to be convicted of any crime to be placed on it, and there is no way to challenge gang designations. Criteria for designation include "living in a known gang area" and "association with gang members."

People who are labeled as gang members are targeted for harassment and abuse by police. They are charged with inchoate crimes and crime by association, rather than the commission of specific acts, and are held pre-trial for years on the basis of those associations alone. Massive NYPD resources are spent building cases in back rooms instead of improving the lives of young people and their communities. Gang policing criminalizes affiliation with friends, relatives, and neighbors without achieving community safety. This practice is costly in both human and fiscal terms.

According to the Grassroots Advocates for Neighborhood Groups and Solutions (G.A.N.G.S.) Coalition, between 2003 and 2013 about 30% of people added to the database were children, some as young as 12. The NYPD continually expands the ways that someone can be added to their catalog. The database is also riddled with errors. BDS has represented numerous people who are incorrectly identified as gang members; others are misidentified as belonging to a certain group.

Even in instances where the database correctly identifies someone as a gang member, police cataloging of young people does not enhance community safety. The NYPD surveils children and young adults, sometimes for years, without alerting parents that their children are being surveilled or investigated. Mass surveillance, such as through the Domain Awareness System (DAS) and these types of covert gang operations, commands enormous budgetary expenses without measurable improvements in safety.

Almost five years ago–in unplanned unison with inspectors and auditors in several other major cities–the OIG-NYPD opened an investigation into the NYPD's Gang Database. Those other inspector general and auditing offices have long since published eye-opening reports documenting the harms, inaccuracies, and broad deleterious social impacts of gang databases.[7]

[7] *See, e.g,* The City of Chicago's Office of Inspector General, *Review of the Chicago Police*

Meanwhile, the OIG-NYPD has yet to publish its report and will not commit to a firm publication date. The Office has publicly acknowledged since 2021 that it was either in the final stages of its investigation or had actually concluded its investigation and drafted its report, but the published report remains unavailable somewhere within DOI. During her testimony before the Council on Monday, the Commissioner acknowledged that she had been provided with a draft of the report within her earliest days in office. However, she refused to commit to a certain release or publication date, saying only that the report would be issued within the year.

It is well past time for the OIG-NYPD to release its report. It is also well past time for the City Council to act to address the inappropriate political pressures being placed on this allegedly independent oversight office, the unconscionable delays being erected by the NYPD and others, and the abysmal pace of the Office's investigations and reporting.

Even without the OIG-NYPD's final report, the City Council should move to eliminate the Gang Database and to rein in horrifically abusive and violative NYPD gang policing practices.

2. NYPD's purchase, development, and deployment of new tools

In 2021, through the work of the Legal Aid Society, it became public that the NYPD had purchased a large number of surveillance tools and technologies using an unregulated slush fund called the "Special Expenses Fund."[8] Wired reported: "The secret purchases stem from 2007, when officials in the comptroller's office, the Office of Management and Budget, and the NYPD crafted a 'memorandum of understanding' that permitted the NYPD to withhold contracts for tools used in 'confidential operations' from public scrutiny or city council approval."[9]

However, this latest public disclosure of NYPD's secretive acquisition and development of surveillance technologies was not unusual or new. In fact, for more than a decade, it has been clear that the NYPD has entered corporate partnerships,[10] as well as procured numerous high-tech tools using NYPD Foundation funds to avoid public scrutiny or city council approval.[11] The OIG-NYPD has not conducted a single investigation into NYPD's technology procurement practices.

More troublingly, beginning in 2008, the NYPD leveraged a partnership with Microsoft to build "the complex surveillance platform called the Domain Awareness System."[12] "Developed in direct

---

Department's "Gang Database" (April 2019) (publishing its report in early 2019, Chicago's investigation into CPD's gang database began when the Public Safety section became operational in 2017); California State Auditor, *The CalGang Criminal Intelligence System: As the Result of Its Weak Oversight Structure, It Contains Questionable Information That May Violate Individuals' Privacy Rights*, Report 2015-130 (Aug. 11, 2016) (publishing its audit in mid-2017, California's state auditor began its investigation of CalGang in 2015).

[8] Sidney Fussell, "The NYPD Had a Secret Fund for Surveillance Tools," Wired.com (Aug. 10, 2021).

[9] *Id.*

[10] George Joseph and Kenneth Lipp, "IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color," The Intercept (Sept. 6, 2018).

[11] Laura Nahmias, "Police foundation remains a blind spot in NYPD contracting process, critics say," Politico.com (July 13, 2017).

[12] Elizabeth Daniel Vasquez, "Opinion: Reining in the NYPD's Use of Surveillance Technologies," CityLimits (Feb. 22, 2022).

response to 9/11, the DAS aggregates all surveillance, policing, and intelligence information which the NYPD accesses or generates, regardless of source. The DAS includes sealed records, closed-circuit video footage from cameras located all over the city, and social media information for children as young as 12, among many other data points. NYPD officers then use the system to search all of that information—for any reason—and to generate predictions based on that data."[13]

While the DAS was originally a carefully restricted counter terrorism tool,, the NYPD soon turned the DAS into a mobile application for general policing. By 2016, every NYPD officer could access the DAS on their department-issued cellphones and, later, in-car tablets.

Despite this roll-out occurring *after* the creation of the OIG-NYPD and despite repeated public complaints about the DAS's civil liberties implications, the OIG-NYPD has conducted no investigation into the policies, procedures, deployment, or use of the DAS. The only governmental entity to conduct any kind of audit of the program was the Comptroller's Office in 2015, prior to the full-scale deployment of the system.[14] That limited audit revealed a number of troubling issues with the DAS, including that people who were no longer employed by the NYPD retained credentials to access the system and that the Integrity Control Officers allegedly responsible for monitoring DAS user activities received no set guidelines or guidance on the criteria for their reviews.

It is well past time for the OIG-NYPD to seriously engage with the NYPD's procurement, creation, deployment and use of surveillance technologies. The drumbeat of public alarm across this sector should have been enough to draw the Office's attention, but to ensure true responsibility in this area, the Council should consider amending Local Law No. 70 to make the Office's responsibilities, powers, and independence to pursue investigations in this space more explicit.

3. Property seizure

Many people are victimized by racist and classist police practices such as constant police presence in their neighborhoods, surveillance, pretextual car stops, and routine stop-and-frisks. An often-overlooked element of these police interactions is the common NYPD practice of seizing property, particularly cellphones, from New Yorkers, oftentimes repeatedly and without legal authorization. While these seizures implicate New Yorkers' well-established Constitutional rights to be free of governmental theft and unreasonable search and seizure, they also implicate New Yorkers' privacy interests. TheNYPD's technical capabilities to examine and extract the contents of those cellphones raise serious concerns about the NYPD's agenda in systematically seizing them.

These seizures occur whether or not the owner is ultimately prosecuted for, or even accused of, criminal conduct. We know that phones and other items are routinely taken from victims and witnesses, as well as from people whose arrests were deemed faulty by prosecutors. Property is taken when it has no connection to alleged criminal conduct, and it is kept and sometimes sold by

[13] *Id.*

[14] NYC Comptroller, *Audit Report on the Information System Controls of the Domain Awareness System Administered by the New York City Police Department* (June 26, 2015).

the police after they have stonewalled the rightful owner attempting to secure its return. **Furthermore, we have every reason to believe, given the NYPD's data capabilities and the testimony of cellphone and laptop owners about the state of their items after police seizure, that the NYPD is using its unchecked power to seize property as a warrantless and illegal intelligence-gathering tool**.

The Police Department's Property Clerk division has long kept custody over any property seized by police officers from citizens. The entirety of the Property Clerk's authority is derived from Section 14-140 of the City's Administrative Code. There is no state statute bearing on the matter. There is no meaningful check on property retention by New York City police as part of the criminal process.

This local ordinance has been outmoded for many years and is in serious need of sweeping reform. It dates back to the 1940s. In the law's current form, the police regularly take away a person's property, often, but not always, as part of an arrest of the person or of a family member. The process by which a person can recover such seized property is confusing to unrepresented people, and completely lacking in basic due process.

We urge the City Council to support a robust legislative response to this harm and not just simply create new rules for the NYPD to decline to follow.

- **Hundreds of thousands of New Yorkers are impacted by property seizure every year, with police failing to return personal property to nearly half of them.**

Police disproportionately target Black, Latinx, and low-income people for stops, searches, and arrests.[15] The people who are most likely to encounter the police, and thus the most likely to have their property seized, are also the most likely to be subjected to police violence.[16] This makes it challenging–and potentially dangerous–for them to intentionally engage with police, as would be required to retrieve their property. These same people are also the least likely to be able to afford legal assistance or replacements for expensive items such as cellphones. The NYPD practice of property seizure compounds the racial and economic inequities inherent to policing in our City and throughout the nation.

The NYPD released official data on citywide property seizures from 2020 as mandated by Administrative Code 14-169.[17] The data, while striking, marked a continuation of trends from prior years for which there is available data. While fewer total items were taken, about the same

[15] Data from the Legal Aid Society from 2019 showed that nearly all people who were stopped and frisked by the NYPD—a practice that persists despite extensive litigation—were people of color, accounting for 90%. In Kings County, where our organization is located, a 2019 report showed that 86% of all people charged with crimes in the borough over a six month period were people of color.

[16] The New York Times, "Why Was a Grim Report on Police Deaths Never Released?" https://www.nytimes.com/2020/06/19/opinion/police-involved-deaths-new-york-city.html

[17] New York City Police Department, Report: Seized Property, available at: https://www1.nyc.gov/site/nypd/stats/reports-analysis/seized-property.page.

percentage was returned. For example, in 2020, the NYPD took 55,511 phones and returned only 33,851. They took 99,986 items of clothing and returned less than half. They took 38,602 forms of identification and returned about one third.. More than 300 vehicles taken for "safekeeping," having no evidentiary value, were never returned. Roughly $81 million in cash was forfeited through the offices of the city's five District Attorneys.[18] More cash was taken and never returned to the owners. The NYPD netted $425,967.50 in the sale of items other than vehicles on the police auction website Propertyroom.com, the proceeds of which went to the NYPD pension fund.[19] Many more items, as we know from our experience, were taken and simply never cataloged.

- **The "process" for property retrieval is unreasonable, arbitrary, and unpredictable.**

As defense attorneys, we can attest that we—trained advocates and lawyers—find the NYPD's property return "process" taxing, time-consuming, frustrating, and ad hoc. Even more dauntingly, this issue very often leaves people to navigate this system without legal counsel. Victims and witnesses of crimes, specifically shootings, have their phones seized by police but are not provided with legal assistance to fight for their return. In an exercise of pure legal fiction, people whose cases district attorneys decline to prosecute—meaning these individuals are never arraigned and thus never connected to a defense attorney, and their cases are never docketed and thus never assigned to a prosecutor—are still required by the NYPD, impossibly, to provide a docket number and receive a release from the prosecutor on their non-existent cases. People who are detained, searched, and released similarly cannot provide required documentation for their belongings. Those who can provide such documentation, usually at the conclusion of their case, are often no better off.

The NYPD also requires that a person come to collect their belongings themselves and will not release property to legal counsel. This policy invites confrontations with officers who wrongly insist that the items cannot be returned. People who have histories of police-related trauma, including the instances where their property was seized without cause, are required to advocate for themselves with members of the NYPD who create arbitrary, inconsistent, and sometimes impossible requirements for property to be returned.

While much of the NYPD practice related to property seizure is targeted and intentional, people attempting to retrieve their belongings are also subjected to incompetence and capriciousness—sometimes being sent on wild goose chases to various NYPD property clerks before being

[18] While there is a criminal forfeiture statute in NY (N.Y. Penal Law § 480), most of this is surrendered through plea agreements whereby defendants agree to "forfeit" cash seized at arrest as part of a plea. Without this "voluntary" surrender of cash the DA has a very high burden to meet for criminal forfeiture and it is only applicable to certain felony drug convictions.This $81 million is not to be confused with civil cash forfeiture litigation pursued by the NYPD. The civil forfeiture secured by District Attorneys are often in small amounts recovered by police from an arrested person's pockets or belongings and are achieved through common cash-for-disposition schemes, where a person will surrender their right to pursue the return of their property or cash in exchange for a more favorable plea or case outcome.

[19] New York City Police Department, Repor:t Seized Property, available at: https://www1.nyc.gov/site/nypd/stats/reports-analysis/seized-property.page.

informed that their property is gone without a trace. Many people are forced to abandon their property after multiple visits, having been sent on a stressful and fruitless quest that proves disruptive to work, childcare, school, and other considerations. As we can attest, the NYPD is not particularly good at keeping track of cash, valuables, and other items that come into their possession. People arrested wearing gold chains or jewelry will be told that their items were never vouchered, and those items are never seen again. People whose phones were documented as being seized by police will be told that they are no longer in NYPD possession, with no information as to the items' whereabouts. Their only recourse is to file suit in small claims court, a time-consuming process where no legal counsel is afforded and where, as in criminal proceedings, the NYPD,with its vast resources, enjoys a significant advantage.

- **The NYPD seizes and keeps items regardless of their alleged connection, if any, to criminal conduct by the owner.**

As discussed above, the NYPD takes items from people regardless of the reason they are being confronted by the police. Whether or not someone is accused—not to mention convicted—of a crime, their property is often seized by members of the Department. We often speak with people who come to us for help retrieving their property. The circumstances vary widely, but a common thread is the frustration they feel at the lack of responsiveness and responsibility from the NYPD and prosecutors.

While the justification for seizing property incidental to an arrest is the need to obtain and preserve evidence needed in a criminal prosecution, it is the NYPD, not the prosecutors, who determine how property will be vouchered and, as a result, what rules will govern its retention and return.

One might presume that property held as evidence in an ongoing criminal prosecution would be the most difficult for an owner to get back. Yet except for property vouchered for "safekeeping" – returnable as soon as the owner appears with sufficient identification— "arrest evidence" is the least contentious category the NYPD currently uses. While the hoops a defendant must jump through to retrieve property vouchered as "arrest evidence" are still substantial and confusing, there are regulations laying out procedures and deadlines governing the process for requesting and obtaining a district attorney's release and for demanding property's return from the property clerk. In contrast, a growing number of New Yorkers are struggling to retrieve property vouchered as "investigatory". This designation, seemingly created out of thin air to circumvent the burdensome due process that accompanies retention of property vouchered as evidence, is alleged to be a justification to retain property indefinitely without court order and without oversight. Phones, clothing, and other property are often held for months without any prosecutorial involvement and the NYPD's "procedures" dictate that the only remedy is to convince the arresting officer to change the property's designation to safekeeping manually. No other personnel at the NYPD or the law department will concede anyone else has authority to mark the investigation as concluded or release the property.

It is essential that the imposition of any new rules be both enforceable against the NYPD and crafted to avoid burden-shifting to the person whose property has been taken, such as by creating

avenues of relief where the onus is on the aggrieved party to follow up, show up, and fight an intransigent bureaucracy.

- **What the NYPD does with technology in their possession is shrouded in secrecy.**

Since approximately 2018, the NYPD has had the technological capability to break into electronic devices, particularly cellphones, regardless of the password or encryption status of those devices.[20] Two spytech companies—GrayShift and Cellebrite—provide tools that allow law enforcement to crack almost any cellphone.[21] Those same companies, amongst others, also sell tools that will create complete digital images (i.e. a precise copy) of a device's contents. These tools not only copy the direct physical items saved on the device (e.g. photos taken by the cellphone), but also can copy data that is stored in applications or in the cloud (e.g. Facebook data, Google Maps data, or Apple iCloud data).[22] The NYPD routinely uses digital forensic tools to image cellphones and other digital devices.

As the United States Supreme Court recognized in 2014, "[a cell] phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form." *Riley v. California*, 134 S.Ct. 2473, 2491 (2014). That information is available to the NYPD from every seized phone in a matter of minutes. As long as the NYPD does not attempt to directly use seized information in a criminal prosecution, but instead only uses that data for intelligence gathering, database construction, and investigative leads, no court process regulates the NYPD's digital search capabilities. Even if the NYPD returned digital devices that had been imaged, as long as they did not encounter some form of technical error, it is not as if those devices would display a message (or retain any clear indication) that they had been cracked or imaged.

Without true accountability and transparency around NYPD's activities involving seized digital devices, like phones, we (as defenders) are left only with what is known about the department's capabilities (as discussed above) and the alarm-raising reality that officers are routinely and unjustifiably seizing digital devices from our clients and communities.

4. Surveillance technology errors and malfeasance

Not only should the OIG-NYPD be examining the systemic deployment of surveillance technologies and analytical systems, but the Office should also be a watchdog for technological error and malfeasance:

---

[20] Agreement to Provide Gray Key Device and Licenses for the New York City Police Department, dated Aug. 17, 2018, available at https://www.documentcloud.org/documents/20392994-18s119-executed-agreement-with-redactions-accepted_redacted-legal-10897172.

[21] Jack Nicas, "The police can probably break into your phone," NYTimes (Oct. 21, 2020), https://www.nytimes.com/2020/10/21/technology/iphone-encryption-police.html

[22] Logan Koepke, Emma Weil, Urmila Janardan, Tinuola Dada, and Harlan Yu, "Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones." Upturn (Oct. 2020), https://www.upturn.org/reports/2020/mass-extraction/.

- **Shotspotter**

In 2021, after an independent investigation conducted by journalists and academics, the Chicago Office of Inspector General's Public Safety Section acted on the reported inquiry and data and conducted an investigation into the accuracy and deployment of the ShotSpotter system in the City of Chicago.[23] The Chicago OIG concluded: "from its analysis that CPD responses to ShotSpotter alerts can seldom be shown to lead to investigatory stops which might have investigative value and rarely produce evidence of a gun-related crime. Additionally, OIG identified evidence that the introduction of ShotSpotter technology in Chicago has changed the way some CPD members perceive and interact with individuals present in areas where ShotSpotter alerts are frequent."[24]

The technology deployed in New York City is identical to that deployed in Chicago. NYPD's public statements regarding ShotSpotter's deployment here–namely that deployment targets "high crime areas"–mimics precisely the Chicago Police Department's statements about deployment. The OIG-NYPD should be conducting a similar investigation into the accuracy and deployment-decision impact on biased policing of New York's ShotSpotter investment.

- **Clearview AI technology**

In April 2021, Buzzfeed broke the news that despite NYPD's public assurances that the Department had never formally contracted with the controversial facial recognition company Clearview AI,[25] documents obtained by the news outlet indicated that the NYPD's public statements had been misleading at best.[26] Those records revealed that the NYPD *had* included Clearview AI amongst its list of acknowledged vendors, beginning in 2018, and that NYPD officers had independently set up and used promotional accounts from the company to conduct unmonitored, undocumented, and unregulated facial recognition analysis in their cases.[27]

In light of these disclosures alone, the OIG-NYPD should be conducting an investigation into the NYPD's public misstatements about their relationship with Clearview AI, the extent of the actual relationship, the extent of NYPD officer use of the technology, and the failures of NYPD policy to regulate and manage NYPD use of facial recognition technology in cases.

- **NYPD's access to DOC's Securus databases, including attorney-client call recordings**

[23] The City of Chicago's Office of Inspector General, *The Chicago Police Department's Use of Shotspotter Technology* (Aug. 2021).
[24] *Id.*
[25] Kashmir Hill, "The Secretive Company that Might End Privacy as We Know It," NYTimes (Jan. 18, 2021).
[26] Caroline Haskins, "The NYPD Has Misled the Public About Its Use of Facial Recognition Tool Clearview AI," BuzzfeedNews (April 6, 2021).
[27] *Id.*

In March 2021, it became public that the City's Department of Corrections illegally recorded more than 1,500 privileged calls between people incarcerated in its jail and their attorneys c.[28] In addition to this illegal recording project, which was facilitated by Securus Technologies,[29] it was revealed that those illegal recordings had been shared with District Attorney's offices throughout the City, as well as with the NYPD.[30]

This breach of New Yorkers' constitutional rights should have sparked an immediate investigation by the OIG-NYPD into the illegal recording program, as well as what recordings were obtained by the NYPD, what access the NYPD has departmentally to Securus's call recording databases, and the policies and procedures in place to regulate NYPD access, use and reliance on those recordings.

5. Forensic laboratory mistakes and malfeasance

In addition to these needed areas of technological oversight, the OIG-NYPD should also be exercising its authority to audit and review the repeated scientific mistakes and malfeasance occurring in the City's law enforcement-related laboratories. Two examples:

- **Coding errors affecting thousands of drug cases**

In March 2021, the NYPD's Police Laboratory notified its accrediting body, ANSI National Accreditation Board (ANAB), that a coding error in NYPD's in-house manipulation of purchased analytical software had resulted in a bug. The NYPD's error was introduced into the program's code in fall of 2016, but was not caught until March of 2021. For five years, the coding error caused NYPD Controlled Substances Laboratory reports to display incorrect values for test results.

In other words, while blatantly asserting that the error did not impact the accuracy of casework, the Laboratory reported that false reports had been issued in all cases involving mass spectral data printouts for a period of *five years*.

These errors were introduced to the system by the NYPD's manipulation to the source code of a purchased software package. The purchased software package produces a robust set of forms, charts, and data for printing and disclosure to reflect the testing and analysis conducted within the package. However, in the interest of efficiency and, perhaps, reduced transparency, the NYPD's Lab chose to edit the software's code to curate the forms, charts, and data produced, reducing the volume of printing and disclosure to a handful of pages instead of the full documentation. It was

[28] Elizabeth Daniel Vasquez, "Dismantle NYC's Mass Surveillance Project – Start with Jail Recordings," TruthOut (June 1, 2021).
[29] Securus Technologies is a purported prison telecom company that makes its profits off of marketing, selling, and deploying a broad set of surveillance technologies. New York City's pension funds are the single largest investor in Securus Technologies.
[30] Chelsea Rose Marcius, "NYC's 5 DA offices wound up with recordings of confidential jailhouse calls between inmates and lawyers," NYDailyNews (March 22, 2021).

this effort to reduce disclosure that introduced the error and caused false data to be disclosed across thousands of cases.

More troublingly still, though the lab's protocols require analysts to review the line of data that was affected by the coding error in their analysis, the coding error went unnoticed for *five* years.

The OIG-NYPD should be conducting an investigation into the NYPD's curation of drug-testing related disclosures, the policies and procedures that allowed for the introduction of this coding error, the failure of the lab's quality assurance processes to catch this error, and the true impact of this error on justice in New York City's criminal legal system.

6. NYC's rogue DNA database

In 1997, the New York City Office of Chief Medical Examiner (OCME) implemented a system for collecting previously-typed DNA profiles into a searchable local database. Originally, the OCME's local database was called LINKAGE. In 2014, the lab absorbed the LINKAGE database into the local level of the CODIS database,[31] called the Local DNA Index System ("LDIS").

Meanwhile, at the state level, the New York State legislature had created the State DNA Databank in 1994 with the passage of Executive Law § 995. That database became operational in 1996. By law, when it comes to known contributors, the New York database can only house DNA collected from people convicted of a crime. While the list of crimes for which a conviction permits DNA sample collection has grown five times since 1996, the New York State legislature has repeatedly rebuffed efforts to expand DNA collection to people who are arrested but never convicted of a crime.[32]

Despite New York State's careful balance between the individual's rights to genetic and basic privacy, as well as due process, and the State's interest in crime solving, the City of New York's agencies—the NYPD and the OCME—have chosen to operate a rogue DNA database that reaches samples taken from persons not authorized for collection. In other words, the OCME's "LDIS"

[31] By way of brief background, CODIS (Combined DNA Index System) is actually the software databasing package developed and provided by the Federal Bureau of Investigation to DNA laboratories around the country. The CODIS database system consists of three levels: the National DNA Index System (NDIS); the State DNA Index System (SDIS); and the Local DNA Index System (LDIS). As the administrator of the CODIS database system, the FBI promulgates detailed regulations governing the types of samples that can be uploaded to NDIS, as well as quality assurance standards for labs conducting testing that feeds into NDIS.

[32] It is worth noting that, in 1999, the legislative record reflects that then-Mayor Rudy Giuliani even specifically requested that the legislature expand collection to arrestees. Mayor Giuliani asserted: "While the City enthusiastically supports this legislation and acknowledges the positive effect it will have on solving crime, it should be noted that the City of New York believes DNA testing upon arrest would allow for even greater efficiency and effectiveness in law enforcement. Examining DNA samples at the time of arrest would dramatically increase the ability of police to accurately identify or negate one's potential culpability while under arrest." The New York State Legislature refused to expand the database to arrestees.

does an end run around New York State's carefully prescribed scheme. Over the last five years, the OCME's rogue database has been growing.[33]

The expansion of this rogue database began in the years *after* the creation of the OIG-NYPD. Despite repeated legal challenges brought in individual cases, multiple news articles raising alarms about the database, City Council hearings, and now a large-scale class action against the City, the OCME and NYPD's rogue database has never been investigated by any civilian oversight body, including the OIG-NYPD.

- **Growth of the OCME's Rogue Database**

This unauthorized database has been fed in part by the surreptitious collection of individuals' saliva samples by the NYPD. We have watched videos where our clients have asserted their right to counsel as they drink from a water bottle or smoke a cigarette offered to them by the police. NYPD has even been observed offering teenagers cigarettes in addition to juice bottles or water bottles for DNA collection. No person, let alone a child, would envision that accepting a cigarette to smoke in the middle of a public building with the blessing of the police would mean that their DNA profile would end up in perpetuity in a database. Then they are led out of the interrogation room, the cigarette butts and juice bottles are left in an intentionally placed ashtray or garbage bin. The police then collect the cigarette butts and bottles for evidence. This same game plays out with water cups and juice or water bottles, and DNA profiles are collected by the thousands.

The local database is in contravention to Executive Law § 995-d, which dictates that the results of DNA testing are confidential, and which specifically protects the right of a defendant to nondisclosure of his or her DNA information.

As Dr. Howard Baum, former Technical Leader of the OCME and creator of the local database, has stated: he never envisioned that the database would become the repository of profiles that the NYPD dragnetted from Black and brown communities. Our clients have been directly impacted by dragnets – the systematic search for someone such as "a Black male in Brownsville" — practices that target our clients particularly because they are Black or because they are male or because they reside in a particular neighborhood.

Dr. Baum never envisioned that the database would include thousands of profiles from people who were tricked into handing over their DNA without consent or court-order. He never envisioned that the local database would include people who were merely detained – sometimes never even arrested, and many never convicted of any crimes. Even our clients who consented to have their DNA taken have told us that they had no real understanding that their cooperation meant that their DNA would stay in a government database forever.

The local database was also set up long before DAS was created by the NYPD and Microsoft to aggregate data collected by the NYPD across the city. While the DAS's role in aggregating

[33] Ann Givens and Robert Lewis, "Push to solve gun cases fuels rapid growth of New York's DNA database," New York Daily News (Sept. 25, 2017), at https://www.nydailynews.com/new-york/nyc-crime/push-solve-gun-cases-fuels-growth-new-york-dna-database-article-1.3516711.

surveillance camera video is well known, another DAS function is its ability to inform officers whether or not an individual detainee's DNA profile is in the database – thus making the detainee a target for DNA collection by individual police officers.

- **The OCME and NYPD DNA Collection and Storage Practice's Threat to our Community's Liberty is Growing**

The current practices of the NYPD mean that it is not only the countless numerical profiles of mainly people of color that are warehoused in an electronic database. For each of those warehoused profiles, the OCME maintains extracts of the DNA in tiny vials. As technologies emerge, law enforcement and the lab can go back to that vial and effectively interrogate the DNA to invade the genetic privacy of the individual's genetic code in even deeper and more disturbing ways.

Genetic genealogy, which has been much reported-on in the news recently, is only the latest incarnation. This technique uses DNA analysis methods that mine more of the human genome for sensitive information than a traditional forensic DNA test and surveil not just the individual's DNA but also the DNA of that individual's entire family line.

The DNA technique employed in genetic genealogy—Single Nucleotide Polymorphism (SNPs) testing or Next Generation Sequencing—is now being considered for widespread forensic uses by the law enforcement community. Whereas traditional DNA testing—Short Tandem Repeat (STR) testing—only measures the lengths of certain segments of non-coding regions on our genome, SNPs and NextGen testing actually code the genome (revealing the specific As, Gs, Ts, and Cs we all learned about in high school) and potentially reveal deeply intimate details including things like predisposition to disease and susceptibility to addiction. And where STR testing only looks at a very small percentage of the overall genome, SNPs testing looks at huge percentages of the overall genome, revealing the most private elements of ourselves.

In the face of this brave new world of genetic testing and the overall threat to privacy, as well as our First Amendment associational freedoms, we need to think about historically targeted communities when considering emerging technologies. The OCME and the NYPD, without oversight or regulation are effectively building a warehoused library of entire communities' genetic extracts. With emerging technologies like genetic genealogy and so-called Next Generation Sequencing, the genetic privacy of not only the individual but the individual's family will come under surveillance by law enforcement.

We now know that 'Junk DNA' is not really "junk" at all: it can be tied by inference to other areas on the human genome, that in turn can reveal sensitive information like susceptibility to disease.[34] As technologies emerge and forensic profiles become even more revealing of a person's biological status, it is incumbent upon our elected officials to protect the genetic privacy of all people. This includes both ensuring that civilian oversight bodies like the OIG-NYPD actually do their jobs and initiate investigations into mass civil liberties violations like those affected by the rogue DNA

[34] *See* "Statistical Detection of Relatives Typed with Disjoint Forensic and Biomedical Loci," Cell 175, 848–858, October 18, 2018, and "Linkage disequilibrium matches forensic genetic records to disjoint genomic marker sets," PNAS | May 30, 2017 | vol. 114 | no. 22 | 5671–5.

database, but also–in this specific instance–that the Council act to end the local DNA database once and for all.

Conclusion

We thank the Council for holding this hearing, and giving us an opportunity to highlight these issues in science and surveillance oversight and the role of the OIG-NYPD. We urge the Council to use every mechanism in your power to dismantle NYPD's sprawling and dangerous surveillance apparatus. We thank the City Council for the opportunity to testify today. If you have any questions or concerns, do not hesitate to contact me at evasquez@bds.org.