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 Technology and Civil & Human Rights

Oversight Hearing on the Use of Biometric Identification Systems in New York City

May 3, 2023

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 Gutiérrez and Williams for inviting us to testify today about the use of biometric identification systems in our city.

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 22,000 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 predominantly low-income and Black and Brown communities bear the brunt of our city’s surveillance ecosystem, carrying a disparate proportion of surveillance load. Biometric identification technologies are deployed in public housing, on our public transit system, in our public benefits programs, and throughout our policing systems from the criminal legal system to the family regulation system and beyond.

I want to thank the Committees on Technology and Civil & Human Rights for holding this important discussion not only on biometric identification systems, but also on their impact on our communities, their relationship to the expanding world of artificial intelligence, and the overwhelming governmental resistance to regulation in this space.

Biometric identification systems are fundamentally a species or outgrowth of artificial intelligence.

This hearing is particularly timely. As public defenders for the borough of Brooklyn, we see these systems in daily use, impacting our clients in the criminal legal systems, the family separation systems, and the immigration systems. We've even seen them deployed against our clients seeking unemployment benefits, facing evictions, or calling their loved ones from detention.

Underlying the mad spread of biometric identification systems is the national and global expansion of artificial intelligence generally. Computerized pattern matching engines are dominating the news and their dangers are being debated globally.

The bills proposed here—Int. 1014 and Int. 1024—address one symptom of this proliferation but they do not ultimately address the underlying disease. To get to the core of this era-defining issue, it is critical to understand how machine learning or artificial intelligence (AI) works.

Fundamentally, to build an AI system, a developer needs a large amount of data. Features of surveillance data—like the faces in surveillance footage—form datasets used by big tech. Those large datasets "teach" AI systems. Without those datasets, biometric identification systems would be impossible. AI, then, brings with it a voracious appetite for data.

Thus, the conversation our community truly needs to have is not one centered around banning individual technologies but instead around defining our rights to our data. And particularly, grappling with the inequities of the data surveillance economy we are already constructing around ourselves.

The single biggest user of biometric identification technology in our city is government.

Agencies as diverse as the NYPD, Department of Correction, the Administration for Children's Services, NYCHA, the Department of Labor, Department of Homeland Security, Immigration and Customs Enforcement and Customs and Border Protection, use biometric identification systems. And the neighborhoods carrying a disproportionate amount of our city's surveillance load are Black and Brown. Strikingly, the bills before the committees today do not directly address these facts.

Our city has invested billions in a twenty-year surveillance infrastructure building program that relies critically on biometric identification technologies. Despite these investments and deployments, the promise of enhanced public safety has not been realized. Instead, all this surveillance infrastructure has accomplished is to expand the burgeoning surveillance state, repeatedly infringe on New Yorkers' dignity, privacy, and First Amendment freedoms, and further entrench the systemic racism inherent in our criminal legal, family separation, and immigration systems. This reality has nothing to do with accuracy or the need for improvement. There is no way to construct a surveillance state in a way that honors our fundamental rights and dignity or builds real justice.

Some examples that exemplify this point:

A. *Voiceprints: Securus Technologies*

In 2018 and 2019, our Council led the country in making phone calls from city jails free of charge. By 2021, however, it became very clear even though calls no longer cost our clients and their families money, these calls carry a far more significant cost.

The first indication of this came when it was revealed that DOC and its phone service and surveillance vendor Securus had illegally recorded more than 1,500 privileged phone calls between people incarcerated and their attorneys. This illegal activity was not new for Securus. Since 2018, they've been sued nationwide for this practice. But illegal call recording turns out to be the tip of the iceberg when it comes to Securus' troubling surveillance scheme.

The company has built a vast and interconnected web of surveillance that is perpetually blanketing not only those presently detained in our city's jails, but also their families, communities, and advocates. For example, Securus houses a database of the audio recordings of every call made from our city's jails, the transcribed text of those calls, the personal information of everyone who has been processed into those jails, and the financial information of every community member who has put money on a commissary account.

That broader database operates on the indexing power of Securus's voiceprint collection and storage. A biometric identifier, voiceprints record the arguably unique signature of a person's speech patterns. To make its NextGen Platform work, Securus collects the voiceprints of everyone who has ever placed or received a call from New York city's jails. The company and DOC do not delete these voiceprints after a person leaves custody—even if they are found not guilty or have charges dismissed.

Presently, Securus's surveillance web, however, is constructed without any court oversight and no need for a warrant. By contrast, if a person was able to afford bail and so was not being held in city jails, law enforcement would only be able to eavesdrop on that person's calls with a specifically-issued warrant. Borrowed or gifted money would not be tracked. And voiceprints would remain a person's private information. Under Securus's system, the mere reality of being poor and unable to afford bail means a detained New Yorker today, along with his or her entire community, has fewer rights, less privacy, and diminished dignity.

It bears repeating, in case the implications of this web are not clear, that more than 80% of those detained are being held pretrial. Convicted of nothing and predominantly held due to an inability to afford bail, those held pretrial are also more than 90% Black and Brown. This web of surveillance is impacting communities of color at a staggering rate.

B. *DNA: OCME/NYPD'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. 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 with the passage of § 995, when it comes to known samples, New York databases 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.[1]

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 legally authorized for collection. In other words, the OCME's "LDIS" 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.

This unauthorized database has been fed in part by the secret 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. But once our clients are led out of that 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 DNA. This same little game plays out with water cups and juice or water bottles, and DNA profiles are collected by the thousands.

Though the local database was also set up long before the NYPD's Domain Awareness System[2] was created, its contents have since been connected to the Domain Awareness System (DAS). While the DAS's role in aggregating 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.

[1] 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.

[2] The Domain Awareness System (DAS) is a software program created by the NYPD and Microsoft that aggregates data collected by the NYPD across the city.

The current practices of the NYPD and OCME 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 individuals' DNA but also the DNA of that individual's entire family line.

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.

C. Faceprints: Clearview AI and the HIDTA backdoor

The NYPD has repeatedly publicly suggested that only the Facial Identification Section of the NYPD conducts facial recognition analysis, that this process is thoroughly documented, and that the analysis is governed by clear rules and protocols. Our experience in cases reveals these public assurances to be false.

The NYPD, in fact, uses two additional avenues to apply facial recognition: officer promotional accounts with Clearview AI and a software backdoor in DataWorksPlus.

In April 2021, Buzzfeed broke the news that despite NYPD's public claims that the Department had never formally contracted with the controversial facial recognition company Clearview AI, documents obtained by the news outlet indicated that the NYPD's public statements had been misleading at best. 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. When those promotional accounts are used by officers in cases, no reports are written, the results are undocumented, and the technology's use is often glossed-over or denied.

But Clearview AI promotional accounts are not the only undocumented avenue for facial recognition use, officers can also use access to PhotoManager (a system used to create photo arrays) to deploy the facial recognition algorithms owned by the High Intensity Drug Trafficking Area (HIDTA) and shared with the NYPD. As with Clearview AI promotional accounts, when officers use this backdoor in cases, no reports are written, the results are undocumented, and the technology's use is often glossed-over or denied.

These examples drive home two critical insights: (1) the "surveillance load" in our city is being disproportionately carried by Black and Brown neighborhoods and communities; and (2) despite the common belief that the courts provide oversight of government tactics, the collection, storage, and use of the vast majority of surveillance data–including biometric data–will never be reviewed by any court or anyone outside law enforcement.

(1) Surveillance load. "Data-driven," "smart" and "intelligence-led" policing methods were created in response to the biased policing of the Broken Windows and stop-and-frisk eras. But they replicate the same racist biases of those periods and fit neatly into the current "New Jim Code" era, in which "new technologies . . . reflect and reproduce existing inequities."[3]

- More than 90% of those whose voiceprints are being taken by Securus Technologies are Black and Brown;

- The OCME/NYPD have refused to disclose the racial composition of the rogue DNA database, but available data suggests the data comes overwhelmingly from communities of color; and

- When it comes to the placement of facial-recognition compatible CCTV cameras, Amnesty International found that "[i]n the Bronx, Brooklyn, and Queens, . . . analysis showed that the higher the proportion of non-white residents, the higher the concentration of [those cameras]." [4]

Scholars have drawn a line from slavery through convict-leasing programs and on to mass criminalization. That line was not miraculously broken by the introduction of AI.

(2) *Court regulation.* As it relates to the courts' ability to oversee the NYPD's use of biometric data, a close examination of the NYPD's POST Act disclosures brings home the devastating reality that court's are not and cannot be the solution. Despite the common belief that the courts provide oversight over police tactics, the collection, storage, and use of the vast majority of the NYPD's surveillance data will never be reviewed by any court or anyone outside law enforcement. According to its own disclosures, the NYPD does not believe it needs to seek a warrant or court approval to use three-quarters of the surveillance collection methods it has disclosed using.

Conclusion

We thank the Council for holding this hearing and giving us an opportunity to highlight these issues in surveillance. In the face of our city's permeating surveillance ecosystem, there is significant urgency for the Council to truly and thoroughly reckon with the use of biometric identification systems. We welcome an opportunity to speak with each of you more about the

[3] Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code*. Oxford, England: Polity (2019).

[4] Amnesty International, *Inside NYC's Surveillance Machine* (2022), https://banthescan.amnesty.org/decode/

breadth of the problem we are seeing in Brooklyn and the comprehensive solutions we have begun to identify from our unique vantage point in the city.

The bills before the Committees today are a step and they would positively impact the communities of Brooklyn that BDS serves, but they are not enough.

If you have any questions or concerns, do not hesitate to contact me at evasquez@bds.org.