Brooklyn Defenders

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

Tel (718) 254-0700
Fax (347) 457-5194
info@bds.org

TESTIMONY OF:

Talia Kamran, Staff Attorney

BROOKLYN DEFENDER SERVICES

Presented before

New York City Council Committee on Technology

Oversight Hearing on Facial Recognition Technology and the Collection of Biometric Data

March 2, 2026

My name is Talia Kamran and I am a Staff Attorney in the Seizure and Surveillance Defense Project at Brooklyn Defender Services. Brooklyn Defender Services (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 Chair De La Rosa for inviting us to testify today about the use of biometric identification technology in our city.

For 30 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. After 29 years of serving Brooklyn, we expanded our criminal defense services to Queens. We represent close to 40,000 people each year who are accused of a crime, facing the removal of their children, or deportation. Our staff consists of 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 and family policing systems and beyond.

BDS Supports the Regulation of Biometric Identification Technology Through Introductions 428 and 213

BDS supports both Introduction 428, which would limit the use of biometric identification technology in residential buildings, and Introduction 213, which would regulate biometric surveillance in places of public accommodation. These bills recognize the urgent reality that the use of biometric identification technology in daily life activities such as entering your home or

shopping for groceries are not neutral innovations that can be imposed on the public without regulation, transparency, and meaningful safeguards. Biometrics broadly encompass unique biological or behavioral characteristics such as facial features, fingerprints, voiceprints, iris patterns, or gait. They are immutable markers of personal physical identity that must be protected as intimately as any other personal information or property. Biometric identification technology refers to systems that attempt to identify or verify a person's identity by analyzing these unique characteristics using automated or algorithmic processes.

Biometric identification technology refers to systems that attempt to identify or verify a person's identity by analyzing these unique characteristics using automated or algorithmic processes. Biometric technology, like all artificial intelligence (AI) tools, must be trained on immense amounts of data. The more data they consume, the more powerful and invasive they become, until they erode individuals' privacy to such a great degree that there can no longer be a meaningful expectation of privacy whether you are buying medicine at a pharmacy or walking to the laundry room in your apartment building. As defenders, we have seen over the last several decades that the more the right to privacy is diminished, the fewer protections people have under the Fourth amendment, leading to a higher risk of legal system involvement, and wrongful convictions.

To Protect New Yorkers, City Council Must Pass Introductions 213 and 428

Introduction 213

The use of biometric identification technology in residential buildings raises serious constitutional and privacy concerns, particularly where access to one's home is conditioned on the surrender of one's biometric information.

These systems are frequently described as "virtual doorman" services and marketed as convenient and harmless. However, secure building access can be achieved through significantly less intrusive means, including key fobs, physical credentials, or regularly updated access codes. Unlike passwords or access cards, biometric identifiers—such as faceprints, palm prints, or voiceprints—cannot be changed if compromised. In the event that biometric data is leaked, there is no way to recover one's identity.

The collection and retention of biometric data in the residential context also implicates First Amendment protections. When landlords maintain access logs with biometric data, they can generate detailed records of tenants' associations, movements, and visitors. The existence of these databases creates risk not only of misuse by private actors, but also of access by government agencies. Immigration and Customs Enforcement's recent uptick in obtaining and purchasing data from private entities underscores the risk of allowing the unregulated

overcollection of personal data.[1] The agency has tracked individuals and circumvented legally required warrant practices with the express objective of facilitating deportation as well as targeting activists.[2]

The Constitution has long recognized the home as being entitled to the highest degree of protection from government interference. And yet, through biometric surveillance in residential apartment buildings, the safeguards afforded by the constitutions such as the warrant requirement for search become meaningless. For these reasons, BDS urges the Council to pass Int. 213.

Introduction 428

The risks to people's privacy and rights are placed at further risk by the use of biometric surveillance broadly in places of public accommodation. In addition to the erosion of individuals' privacy, the use of biometric surveillance in public venues places people of color at risk of discrimination and even false arrest.

Facial recognition technology is widely documented as racially biased and unreliable, particularly for people of color and women. In December 2023, the Federal Trade Commission banned Rite Aid from deploying facial recognition technology for five years after finding the company used flawed AI that falsely identified customers—disproportionately people of color and women—as shoplifters.[3] Acting on thousands of false matches, employees followed customers, searched them, publicly accused them, and in some cases contacted law enforcement.[3]

New York City does not need to wait for a finding of further harm before absorbing the lesson Rite Aid has to offer - the use of frequently inaccurate, highly invasive biometric identification technology does not enhance public safety; it amplifies bias and humiliation and harms consumers, particularly consumers of color.

In light of the serious threat to individuals' privacy, civil rights, and freedom, BDS strongly urges the City Council to pass Introductions 213 and 428.

---

[1] Joseph Cox, *CBP Tapped into the Online Advertising Ecosystem to Track Peoples' Movements*, 404 Media (Mar. 3, 2026), https://www.404media.co/cbp-tapped-into-the-online-advertising-ecosystem-to-track-peoples-movements/ (describing an internal DHS document showing that CBP purchased ad network-sourced location data to monitor phone movements, which can reveal residential locations without a warrant).

[2] NPR, *ICE Has Spun a Massive Surveillance Web. We Talked to People Caught in It*, (Mar. 4, 2026), https://www.npr.org/2026/03/04/nx-s1-5717031/ice-dhs-immigrants-surveillance-confrontation-deportation-mobile-fortify (reporting on ICE's use of Mobile Fortify and related facial recognition tools in law enforcement operations, including concerns that data aggregation and technology deployment bypass traditional warrant requirements).

[3] *FTC*, *Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology Without Reasonable Safeguards*, Federal Trade Commission (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without

The City Must Limit Its Own Agencies' Use of Surveillance Tools That Gather Intimate and Unnecessary Personal Data

While regulating the collection of biometric data in the private sector is urgently necessary, the legislation at issue today does not address the fact that *the biggest user of biometric identification technology in our city is our own city government.* New York City has spent billions over the last two decades building a vast surveillance infrastructure under the assertion that each new invasion of privacy will enhance public safety. Yet despite these investments, the promise of enhanced public safety has not materialized. Instead, what has expanded is the surveillance state in violation of New Yorkers' dignity, privacy, and Constitutional rights.

As public defenders, we see biometric recognition technology systems in daily use, impacting our clients in the criminal legal systems, the family separation systems, and the immigration systems. Underlying the 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. We see AI surveillance tools deployed against our clients seeking unemployment benefits, facing evictions, or calling their loved ones from detention. The bills proposed here 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 AI works. Fundamentally, to build an AI system, a developer needs a large amount of data to "teach" AI systems. Without those datasets, biometric identification technology 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 rights to our data and, particularly, grappling with the inequities of the data surveillance economy we are already constructing.

Securus Voiceprint and Social Network Surveillance

Consider the example of Securus, the company contracted to provide phone call services for New Yorkers who are incarcerated in our city jails. Securus houses a database of every recorded jail call, in some cases even recording legally protected calls between individuals and their attorneys. Worse yet, Securus collects and stores voiceprints, capturing the unique vocal signatures of everyone who has ever placed or received a call from a New York City jail.

These voiceprints are not deleted when a person leaves custody, even if charges are dismissed or the person is found not guilty. Further, Securus's surveillance web is constructed without any court oversight and no need for a warrant. If a person is able to afford bail and avoid 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 that person's private information.

Under Securus's system, the mere reality of being poor and unable to afford bail means a New Yorker who is detained today, along with his or her entire community, has fewer rights, less privacy, and diminished dignity. More than 80% of those detained at Rikers Island are being held pretrial, which means they have not been convicted of anything, and are incarcerated due to an inability to afford bail. And the regime of data collection and surveillance turns on two axes of inequality–income and race. Significantly, more than 90% of individuals in pretrial detention are Black and brown people. Meaning that the data gathered by the Department of Corrections (DOC) through Securus - data shared with other agencies, used to train other AI-enabled surveillance tools - is almost exclusively gathered from low-income people of color.

The harm of the city's use of Securus extends past the fact that data is near-exclusively collected from low-income people of color. That data does not stay neatly within DOC control– Securus operates a platform known as "Threads," which aggregates and analyzes call metadata, voiceprints, billing names, addresses, and other identifying information across the thousands of correctional facilities nationwide that contract with the company. Through Threads, Securus pools data from facilities across jurisdictions and uses analytic tools to map social networks, identify shared contacts, track communication patterns over time, and generate association graphs. In effect, information from calls into or out of New York City jails is integrated into a nationwide database designed to reveal relational and behavioral patterns across institutions, threatening the privacy of anyone who contacts an incarcerated person. Threads interacts with other data platforms and has integration capabilities with Palantir, the surveillance and analytics corporation building interoperable databases to track immigrants, raising concerns that jail call data could be accessible to federal immigration authorities despite New York City's sanctuary laws.[4]

Engaging in the deeply human act of supporting someone in custody, something shown to reduce recidivism and improve outcomes, should not result in a person facing police surveillance. For these reasons, in order to protect New Yorker's digital identities and privacy, City Council must also pass Int. 96, the End Community Correctional Surveillance (ECCoS) Act, to ban the recording of jail phone calls and end the invasive and inappropriate surveillance of incarcerated people and their loved ones.

The NYPD Gang Database and Data-Driven Policing

The harm of biometric and other data collection through Securus does not exist in isolation. The skewed data collected through Securus calls is one of many used to build the modern surveillance infrastructure that threatens New Yorkers' Constitutional rights. Each invasive tool

[4] Gwynne Hogan, *ICE May Still Have Massive Access to Rikers Island Data Despite City's Sanctuary Status*, Documented (July 2, 2025), https://documentedny.com/2025/07/02/ice-may-still-have-massive-access-to-rikers-island-data-despite-citys-sanctuary-status/

feeds into other datastreams, like the NYPD's Domain Awareness System and requisite databases. As we have testified in our advocacy to abolish the NYPD's gang database, the NYPD's appetite for data to populate and justify its intelligence systems has led to coercive phone seizures, social media scraping, and the mass labeling of Black and Latine youth within the NYPD Criminal Group Database (widely known as the gang database) based on association rather than conduct.

The NYPD's gang database is part of the technological evolution of broken windows policing—transforming a regime of racially disproportionate street stops into one of racially disproportionate data collection, following the same trend of skewed collection present in the Securus context. Where officers once relied on physical stops and interrogations, they now use surveillance technology, secretive databases, and digital monitoring to track and criminalize Black and Latine youth. This shift does not make policing less discriminatory or less harmful; it simply makes it harder to challenge the basis for a stop or search in a criminal proceeding. Our courts are equipped to examine officer conduct and decisions regarding arrest and investigation as part of the constitutional guarantee that a person will only be arrested based on probable cause. However, when an officer relies on a database designation or algorithmic flag to justify a stop, search, or arrest, the database itself cannot be subjected to the same adversarial scrutiny, if its use is even introduced in court at all.

The gang database extends and deepens the NYPD's long-standing patterns of racialized policing, embedding them into data systems that follow young people indefinitely, regardless of whether they have ever committed a crime.

The injustice of the database ranges from the harm of racial discrimination to severe due process harms. Once a person is designated as a gang member by the NYPD, they have no means to challenge that label in court or elsewhere. This "gang" designation often results in higher bail amounts, increased pre-trial incarceration, and the inability to access much needed programming. Even if a person's charges are dismissed or they complete a sentence, their name remains in the database, leaving them vulnerable to continued police scrutiny and abuse. Unlike unlawful stops and searches, which can sometimes be challenged in court, gang designations offer no pathway for removal, making them a tool of unchecked policing with no oversight.

The transition from widespread stop-and-frisk to expansive data policing has not reduced racial disparities; it has only made them more insidious. The people we represent experience persistent police scrutiny, unjustified stops, and coercive interrogations simply because they live in heavily policed communities. The gang database also causes Black and Latine immigrants to be more susceptible to immigration detention and deportation based on little more than where they live and who they are friends with; this risk of separation from their families and communities is

particularly acute after the recent designation of certain gangs as terrorist organizations.[5] Moreover, young asylum seekers who are fleeing violence from gangs in their home countries are often themselves erroneously labeled as gang members.[6] Given how inaccurate and biased the database is and the risk to people's safety and rights it poses its existence presents an unjustifiable risk of harm.

We do not need this database, and we have ample documentation that it is inaccurate, discriminatory, and easily abused. The NYPD has demonstrated a willingness to bend or break rules to access and share information, and there is no credible way to regulate a system built on such deeply flawed foundations. We call on the City Council to pass Int. 96 to abolish the highly discriminatory and harmful NYPD gang database.

New York Needs Comprehensive Data Protection Legislation, Not Piecemeal Defense Against Data Collection

Taken together, Securus, the gang database, and the rapid expansion of private facial recognition systems demonstrate that AI-powered surveillance tools impose social and institutional costs that should cause us to seriously rethink their rapid acquisition and use in the private and public sector. The predictive or matching capacity of any AI system depends entirely on the dataset on which it is trained and the inputs it continuously ingests. When those datasets are drawn from systems already shaped by racialized policing, economic inequality, and selective enforcement, they help create surveillance and predictive policing tools that are built from distorted baselines.

In this way, historically skewed data becomes the foundation for future suspicion, creating a feedback loop in which past discrimination is encoded as algorithmic bias. The result is not simply flawed technology, but an infrastructure that both depends upon and intensifies the erosion of privacy and equality. These tools require the continuous extraction of personal data in order to exist, and in doing so they transform human bias into automated decision-making power, embedding inequality deeper into the institutions that govern liberty. For these reasons City Council must seriously consider the harm in unchecked data collection–biometric and otherwise–by the NYPD, DOC, and other government entities as urgently as it addresses the private sector.

New York City has the opportunity to end the game of data privacy whack-a-mole in a more holistic way by passing comprehensive data protection legislation that recognizes personal data as precious personal property, that cannot be bought or sold without our informed consent, or accessed by our government, outside of the bounds of the Constitution. There is no way to build a humane surveillance state. There is, however, a way to build a city grounded in dignity,

[5] Terrorist Designations of International Cartels - United States Department of State, https://www.state.gov/terrorist-designations-of-international-cartels/.
[6] See Jonanthan Blitzer, "How Gang Victims Are Labeled As Gang Suspects," The New Yorker, January 23, 2018, https://www.newyorker.com/news/news-desk/how-gang-victims-are-labelled-as-gang-suspects.

constitutional protections, and racial justice. Passing these bills, while committing to broader data justice reforms, is an essential step toward that future.

We thank the Committee on Technology for your commitment to addressing these issues. If you have any questions, please do not hesitate to contact Jackie Gosdigian, Supervising Policy Counsel, at jgosdigan@bds.org.