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 Committees on Technology and Civil & Human Rights

Oversight Hearing on Privacy Protection in the Digital Age

December 8, 2025

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. We are grateful to the Committees Technology and Civil and Human Rights, and Chairs Gutiérrez and Williams for inviting us to testify about privacy protection in a time of rapid digital information collection.

For nearly 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 recently 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.

Background

New York City has entered a period in which the collection, storage, and analysis of data are built into nearly every interaction a person has with a city agency. In many respects, these systems can serve the public good: automating benefits enrollment, tracking demographic needs, and helping agencies design programs more responsive to the people they serve. But for these systems to remain public goods, the city must confront the unprecedented scale of personal information it now holds. By digitizing many city services, the city now has information that is deeply intimate, such as biometric information and geolocational data, making it increasingly capable for the city to expose every facet of a person's life to inappropriate government scrutiny.

At the same time that city agencies have expanded their data infrastructure, the New York Police Department (NYPD or Department) has quietly embedded itself deeper into city systems. Over the last several years, police presence–both physical and digital–has expanded across agencies serving poor, unhoused, and disabled New Yorkers.[1] As a result, individuals who already face heightened risks of police harassment and violence are now made hyper visible to law enforcement across even more fronts. This entanglement reinforces the school-to-prison pipeline, intensifies the criminalization of poverty, and turns services meant to help New Yorkers into additional surveillance touchpoints.

As public defenders, we witness daily how pervasive data collection and surveillance technologies have also deteriorated the constitutional protections of the people we represent. Inaccurate Shotspotter alerts continue to trigger police responses and arrests without genuine probable cause.[2] Racially biased and error-prone facial recognition systems generate misidentifications that lead to wrongful stops, searches, and arrests. And because the machinery that produces these "leads" rarely enters a courtroom, the individuals subjected to these technologies and the public defenders representing them have no meaningful opportunity to challenge the integrity of evidence rooted in flawed surveillance tools. These technologies operate behind a veil, undermining the core constitutional protections that should protect every New Yorker.

More broadly, the city's growing surveillance infrastructure does not merely target individuals; it maps, categorizes, and criminalizes entire communities. The normalization of stripping low-income and working-class New Yorkers, and particularly New Yorkers of color, of their privacy rights must come to an end. Updating our data protection laws to match the conditions of the digital age is a necessary first step in reversing this trend.

Introduction 1335 and Resolution 783

For these reasons, BDS strongly supports Int. 1335. This legislation takes a critical step by expanding the definition of "personally identifying information" (PII) to reflect the realities of the digital age. Modern identification no longer relies solely on names, addresses, or traditional identifiers. Today, a person can be identified through countless data points: their faceprint, voiceprint, gait, geolocation history, app data, browsing patterns, and more. Int. 1335 recognizes that residents' digital identities are no different than one's physical identity and private effects, and therefore require the same level of protection. This is essential not only to prevent identity theft and commercial exploitation but also to ensure that public-service data collection does not become a gateway to expanded surveillance or unwarranted scrutiny.

---

[1] Katie Honan, Reuven Blau & Yoav Gonen, *NYPD Expands Role in Civilian Agencies as Feds Circle Top Cops*, The City (Sept. 11, 2024).

[2] Brooklyn Defender Services, *Confirmed: ShotSpotter Technology Increases Surveillance and Policing of Black and Latine New Yorkers, While Failing to Reduce Gun Violence: Analysis of Nine Years of Previously Undisclosed NYPD Police Data* (Dec. 4, 2024), https://bds.org/assets/files/Brooklyn-Defenders-ShotSpotter-Report.pdf

BDS also supports Resolution 783, which urges passage of New York State's Data Protection Act. Because data routinely flows between city and state systems, modernizing privacy protections at the state level is critical. Statewide consistency will help ensure that New Yorkers' sensitive information is safeguarded no matter which agency collects or stores it. This legislation is essential because porous information-sharing practices create conditions where data that is unnecessary or inappropriate for certain entities to possess nevertheless becomes available to them. Such leakage quietly erodes the right to privacy and expands the universe of actors with access to deeply personal information, increasing the likelihood of misuse or abuse. In New York City, this concern is especially urgent: as a sanctuary city, any gaps in our data-protection framework risk exposing sensitive personal information for the purposes of federal immigration enforcement.

Taken together, these measures begin the process of bringing New York's privacy laws into alignment with the technologies that shape modern life.

Beyond Data Protection, The City Must Limit the Use of Surveillance Tools That Gather Intimate and Unnecessary Personal Data

While Int. 1335 and Res. 783 take important steps toward modernizing privacy protections, the city cannot respect the fundamental right to privacy without also pulling back the invasive and discriminatory surveillance tools that undermine those very protections. Over the past decade, New York City's investment in police surveillance technology has far outpaced the establishment of modernized civil-rights laws that would recognize our digital identities as part of the "privacies of life" protected by the U.S. Constitution. The NYPD has spent more than a billion dollars on an array of powerful surveillance tools with little oversight or regulation. And even where the city has demanded transparency around data collection and surveillance, the Department has consistently sought to evade oversight and accountability. For instance, the NYPD routinely fails to provide comprehensive reporting on its own surveillance technologies as required under the POST Act. Further, the Department has pursued access and use of surveillance technologies through other agencies to avoid publicizing its surveillance activity. The recent revelation of its covert plan with the New York City Housing Authority (NYCHA) to obtain live access to thousands of residential CCTV cameras shows how readily the department is willing to circumvent public processes and democratic safeguards to expand its surveillance reach. These practices create new fronts of constitutional concern and expose New Yorkers to unchecked, technologically amplified policing that operates outside the limits the law intends to impose.

To protect people's constitutional right to privacy, we must not only protect the data the city collects, but must also prevent the city from collecting data it does not need, particularly when that data is discriminatory, inaccurate, or structurally incapable of responsible use.

Passage of Introductions 798 and 963 To Strengthen Data Protections

One of the clearest examples of why stronger data protections must be paired with limits on police surveillance is the NYPD's gang database. Oversight bodies, researchers, and community

members have long documented that the database overwhelmingly targets Black and Latine youth, many of whom have never committed a crime and have no verified connection to unlawful activity. The criteria now used to justify placement, such as alleged "self-admission" pulled from social media or proximity to others similarly labeled, are unscientific, pretextual, and racially coded. The result is not a tool for preventing violence or improving community health, but a set of dossiers on Black and brown New Yorkers that allows the NYPD to wait, watch, and criminalize people by association.

The harm of allowing police to gather and store intelligence in such discriminatory and inaccurate databases extends far beyond surveillance and street-level policing. For example, we've already seen ICE rely on false gang allegations to justify arrests and deportations. This demonstrates the breadth of the danger: a database built on bad information becomes a pipeline through which inaccurate labels travel to other agencies that wield enormous power over a person's liberty, family, and safety.

Even with legislation such as the New York Data Protection Act, which would help limit data leakage, the mere existence of this repository creates a completely unjustifiable risk. A person wrongfully labeled in the NYPD database as associated with a foreign gang could have that designation passed to ICE, placing them at risk of detention, deportation, or removal to a country where they may face persecution or human rights abuses.

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. The time has urgently come to abolish the gang database in its entirety. City Council must pass Int. 798 to eliminate this harmful and dangerous system.

The concern over excessive surveillance and data gathering extend beyond NYPD surveillance and into the broader criminal legal system. People are losing ownership over some of the most intimate aspects of their identities. Systems like Securus, the jail call recording software used in New York, does far more than simply record calls. The AI-enabled software extracts and stores voiceprints, a form of biometric data that would rightly fall under the expanded definition of personally identifying information contemplated in Int. 1335. Crucially, it is not only incarcerated people whose identities are captured: any family member or friend who calls into a jail has their unique voiceprint taken, even when they are not under investigation. Securus also integrates tools such as Securus Threads[3], which allow correctional staff to analyze the social networks of incarcerated individuals and generate maps of those networks inside and outside of prison. Individuals calling their loved ones may have data from those calls shared with the NYPD, raising the risk that they will be surveilled based on their association with an incarcerated person, in violation of their right to privacy and their First Amendment associative freedoms. This means that people engaging in the deeply human act of supporting someone in custody, something shown to reduce recidivism and improve outcomes, may instead find themselves

[3] Securus Technologies, *THREADS — Investigative & Corrections Analytics*, https://securustechnologies.tech/securusthreads/

under police scrutiny or harassment. This information should not simply be protected as personal information or regulated under a data protection act - it should not be gathered at all. For these reasons, in order to protect New Yorker's digital identities and privacy, City Council must also pass Int. 963, the End Community Correctional Surveillance (ECCoS) Act, to end the invasive and inappropriate surveillance of incarcerated people and their loved ones.

Conclusion

As technology increasingly shapes the operations of government and the daily lives of New Yorkers, it is essential that our laws reflect both the risks and responsibilities of this moment. Our city urgently needs expanded data protection laws, limitations on discriminatory surveillance tools, meaningful oversight over the development of algorithms used by city agencies, and so much more. These changes in our legal framework are not only matters of good governance, they are necessary to preserve the constitutional rights and civil liberties that form the foundation of a democratic city.t

Int. 1335 and Resolution 783 modernize the baseline protections residents need in an era of pervasive digital information collection. Ints. 798 and 963 go further by addressing the systems that pose immediate, well-documented harms to Black, brown, immigrant, and low-income New Yorkers, and by ensuring that deeply personal data is not collected or misused in ways that undermine safety, privacy, or due process.

We thank the Committees on Technology and Civil and Human Rights for their commitment to addressing these issues. If you have any questions, please do not hesitate to contact Jackie Gosdigian, Senior Policy Counsel, at jgosdigan@bds.org.