

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 Public Safety, Technology, Oversight & Investigation and Public Housing

Oversight Hearing on The Use of Surveillance in NYCHA Developments

September 30, 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 on Public Safety, Technology, Oversight and Investigation, and Public Housing, and Chairs Salaam, Gutiérrez, Brewer, and Banks for inviting us to testify about the NYPD's plan to expand its CCTV surveillance throughout the New York City Housing Authority's ("NYCHA") many public housing complexes.

For 29 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. In July 2025, Brooklyn Defenders assumed the criminal defense contract previously held by Queens Defenders. We are proud to now provide excellent legal services in both Brooklyn and Queen. 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 represent live in heavily policed and highly surveilled communities. Low-income Black and brown communities bear the brunt of the New York Police Department's ("NYPD") privacy-destroying and harassing 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" to police gaze through cameras, sensors, microphones, digital scraping tools, and their underlying, mass-aggregating databases like the Domain Awareness System ("DAS"). With the expansion of police-controlled cameras in NYCHA housing, tied to Big Apple Connect ("BAC") Wi-Fi program—a free internet and cable program for public housing residents, the city is now extending that constant surveillance directly into people's homes.

New Yorkers, and directly surveilled NYCHA residents, would not have known about this program at all were it not for investigative reporting.² The city did not disclose that Big Apple Connect was being leveraged to expand the NYPD's live CCTV network until journalists brought it to light. We thank City Council for responding swiftly to that revelation by demanding a halt to the program,³ and we agree that it must be stopped. This program violates the civil rights of NYCHA residents and unjustly places low-income New Yorkers under a microscope of government surveillance.

The NYPD and NYCHA Agreement and Surveillance Program is a Violation of the POST Act

Under the POST Act, before deploying or expanding surveillance technology, the NYPD must publish an Impact and Use Policy (IUP) 90 days in advance and hold a public hearing so that New Yorkers can meaningfully weigh in.⁴ The expansion of NYPD's access to cameras into NYCHA housing clearly constitutes such an expansion: prior to Big Apple Connect, the NYPD maintained 37 livestream camera sites in NYCHA buildings; after the program's launch, the Department reported 68 new CCTV cameras, and testified that it hopes to expand to 1,905 cameras by the end November 2025. This is unequivocally an enhancement of the Department's surveillance capabilities, requiring an addendum to its CCTV IUP.⁵ Instead, the NYPD and

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 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 Zachary Groz, *Adams Quietly Uses Free Internet at NYCHA to Expand NYPD Surveillance*, N.Y. Focus (Aug. 11, 2025), https://nysfocus.com/2025/08/11/eric-adams-nycha-nypd-cameras-surveillance.

³ Zachary Groz, *Councilmembers Demand NYPD Halt Its Public Housing Surveillance Expansion*, N.Y. Focus (Aug. 25, 2025), https://nysfocus.com/2025/08/25/nypd-surveillance-nycha-big-apple-connect.

⁴ N.Y.C. Admin. Code § 14-188 (2025).

⁵ Id. § 14-188(d)



NYCHA initiated the Big Apple Connect-supported CCTV expansion without notifying the public, holding hearings, and without publishing a new or amended IUP. In doing so, the two agencies deprived NYCHA residents of the chance to examine, question, or challenge how their homes and lives would be subjected to new monitoring. The fact that this rollout was announced in stealth is itself emblematic of the NYPD's broader pattern of sidestepping transparency mandates of the POST Act.⁶

Even more troubling is the fact that this expansion is not limited to cameras alone. It is built on a municipal Wi-Fi program, and the public has received no explanation of the NYPD's relationship to that program. Wi-Fi technology itself is capable of surveillance. Academic research and industry applications demonstrate that Wi-Fi signals can be used to detect movement, track occupancy, and map human activity within spaces. The POST Act defines surveillance technology as "equipment, software, or systems capable of, or used or designed for, collecting, retaining, processing, or sharing audio, video, location, thermal, biometric, or similar information, that is operated by or at the direction of the department." The Department has not disclosed the terms of its agreement with NYCHA, nor has it specified what access it may have to BAC data. At minimum, the boundaries of NYPD's authority and use of Big Apple Connect should be clearly spelled out in an Impact and Use Policy.

NYPD Expanded Access to NYCHA CCTV Cameras Violate Residents' Fourth Amendment Rights

The NYPD's planned expansion of CCTV surveillance within NYCHA through Big Apple Connect raises serious Fourth Amendment concerns. In public testimony at today's hearing, the Department stated that it currently has 68 cameras with live-stream capabilities to NYPD officers' phones via the Domain Awareness System application via Big Apple Connect. It intends to scale up to 1,905 by November 2025. With access to this many cameras under a unified system, the NYPD will be able to reconstruct the daily movements of hundreds of thousands of NYCHA residents. That kind of spatial-temporal mapping across doorways, hallways, common spaces, and adjacent walkways enables nearly continuous tracking of individuals' routines and associations.

The Supreme Court has made clear that the Fourth Amendment protects against this kind of prolonged and detailed surveillance. In *Carpenter v. United States*, the Court cautioned that

⁶ Talia Kamran, Testimony before the New York City Council Committees on Public Safety, Technology, and Oversight & Investigation (Feb. 19, 2025)

⁷ MIT Technology Review, How Wi-Fi Sensing Became Usable Tech (2023).

⁸ N.Y.C. Admin. Code § 14-188.



when technology enables the government to achieve "near perfect surveillance, as if it had attached an ankle monitor" to an individual, the Fourth Amendment requires a warrant. More recently, the Fourth Circuit in *Leaders of a Beautiful Struggle v. Baltimore Police Department* struck down a program of aerial surveillance, holding that indiscriminate monitoring of residents' movements across the city violated the Fourth Amendment. The intrusion here is even more acute, because it occurs not in public streets alone but around residents' homes—the place the Court has repeatedly described as "first among equals" in Fourth Amendment jurisprudence. The place the Court has repeatedly described as "first among equals" in Fourth Amendment jurisprudence.

If this program is permitted to continue, the NYPD should, at minimum, be required to obtain a warrant before accessing livestream or archived footage for investigative purposes. Absent judicial oversight, NYCHA residents could be subjected to round the clock, suspicionless monitoring of their daily lives in violation of the Fourth Amendment.

NYPD CCTV Disproportionately Surveils New Yorkers of Color in Violation of their Equal Protection Rights

This expansion also raises urgent concerns under the Equal Protection Clause. NYCHA houses more than 528,000 New Yorkers of whom approximately 44 percent identify as Black and 42 percent identify as Hispanic or Latino. ¹² Against this backdrop, it is clear that concentrating thousands of cameras in NYCHA developments will, by definition, disproportionately target people of color, magnifying the already staggering rates of harassment, suspicionless questioning, and stop-and-frisk practices that NYCHA residents already face. The effect is to transform stop-and-frisk into its digital equivalent, embedding racialized surveillance directly into the homes of New Yorkers of color.

The CCTV expansion was covertly launched, which means the public has no insight into how the NYPD selected its initial CCTV placements or how it intends to expand them. This absence of disclosure is itself a violation of the POST Act, ¹³ but it also prevents New Yorkers from

⁹ Carpenter v. United States, 585 U.S. 296, 297, 138 S. Ct. 2206, 2210, 201 L. Ed. 2d 507 (2018)

¹⁰ See Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 2 F.4th 330, 346 (4th Cir. 2021) Holding that the Baltimore Police Department's use of an aerial surveillance system capable of tracking the movement of all residents in Baltimore while outside, and which retained data on individuals' movement for 45 days, constituted a search under the Fourth Amendment requiring a warrant in order to access to the data.

¹¹ Florida v. Jardines, 569 U.S. 1, 6, 133 S. Ct. 1409, 1414, 185 L. Ed. 2d 495 (2013)

¹² N.Y.C. Housing Authority, *Resident Data Summary 2023* (2024), https://www.nyc.gov/assets/nycha/downloads/pdf/Resident-Data-Book-Summary.pdf

¹³ The POST Act requires the NYPD to disclose the disparate impact of its surveillance technologies. Should this program continue, the Department must, at minimum, publish within its CCTV IUP a full accounting of the disparate impact of this expansion on NYCHA residents. N.Y.C. Admin. Code § 14-188(b)(ii) (2025) (requiring



understanding whether the Department is concentrating cameras in ways that will amplify existing racial disparities in policing. We cannot trust that these cameras are being placed in a nondiscriminatory manner when the NYPD has a storied history of racial discrimination in policing, particularly in NYCHA. Floyd v. City of New York revealed that the NYPD's stop-and-frisk practices deliberately and disproportionately targeted Black and Latino residents. Davis v. City of New York more specifically found that the Department's trespass enforcement practices in NYCHA subjected residents and visitors (overwhelmingly people of color) to unconstitutional stops and arrests. Those rulings reflect what legal advocates and NYCHA residents have long known: that NYPD policing in and around NYCHA has been racially discriminatory and harmful.

This CCTV program must also be understood within this history and the broader ecosystem of NYPD surveillance. Through ShotSpotter, predictive policing systems, license plate readers, the gang database, and technological device seizures, the Department directs its attention disproportionately toward neighborhoods of color. NYPD admitted in their testimony that they can capture screenshots from the video footage and run them through facial recognition systems, providing thousands more images of NYCHA residents for facial recognition databases. This practice also disproportionately feeds surveillance data on NYCHA residents into the Domain Awareness System compared to New Yorkers who don't live in NYCHA, reinforcing a self-perpetuating feedback loop that entrenches the racial bias inherent in these surveillance technologies.

Biased data produces biased results: the more the NYPD trains its focus on communities of color, the more "evidence" it generates to rationalize further surveillance in those same neighborhoods. This harm is not abstract. This expansion means that NYCHA residents of color must live not only with the fear of being followed, stopped, or questioned on the sidewalk, but also with the knowledge that police may watch them in real-time all the way up to their own front doors. By embedding surveillance directly into the architecture of public housing, the NYPD communicates that these residents are uniquely unworthy of privacy and uniquely deserving of suspicion. Such unequal treatment offends the Equal Protection Clause and entrenches a two-tiered system of rights.

each Impact and Use Policy to include "information regarding the potential disparate impacts of the surveillance technology, including whether the surveillance technology is disproportionately deployed in certain communities or has a disparate impact on any protected groups").



Conclusion

The city must end the NYPD's collaboration with Big Apple Connect. A program intended to expand digital access for public housing residents should not be repurposed into a tool for mass surveillance. NYCHA residents deserve the same right to privacy in their homes as every other New Yorker, not to be singled out for suspicionless monitoring. Council should ensure that Big Apple Connect is rolled out as a resource for residents, free from NYPD control or surveillance, and should move quickly to stop this collaboration before it further entrenches discriminatory policing practices.

This program is likely to result in heightened surveillance, police harassment, and a rise in wrongful arrests targeting NYCHA residents. Rather than expanding ineffective and unlawful surveillance, the city should invest in community-based programs that have been proven to reduce crime, such as education, jobs, and healthcare. These approaches address the root causes of violence and build safer, stronger neighborhoods without relying on unlawful surveillance.

We are grateful to the City Council for your timely hearing on this critical issue. If you have any questions about our testimony, please feel free to contact Jackie Gosdigian, Senior Supervising Policy Counsel, at jgosdigian@bds.org.