

# *The Price of Free WiFi*

## *The new frontier of digital surveillance in public housing developments*

Since 2007, the department has spent billions of dollars on surveillance contracts, including New York's Domain Awareness System, a real-time surveillance map of the city procured from Microsoft for over \$1 billion, which unifies into a single centralized network more than a dozen public and private technologies, including camera systems, tracking tools, and biometric devices. This system, the same one that NYPD Commissioner Jessica Tisch stated had been used by investigators to track down and arrest [Luigi Mangione](#), the main suspect in the murder of Brian Thompson, then CEO of the health insurance company UnitedHealthcare — is now receiving live CCTV footage from public-housing buildings through the routers and modems installed to provide residents with internet access.



Now, the NYPD is expanding surveillance significantly by installing video cameras inside of many of the city's 335 public housing projects. There are already 68 video cameras sending live feeds to their local police precinct and, according to Anthony Mascia, Commanding Officer of the NYPD's Information Technology Bureau, the number of cameras across public housing is expected to increase to 1,900 by the end of the year.

As a result, thanks to the agreement with NYCHA, the NYPD can now reconstruct the daily movements of hundreds of thousands of NYCHA residents, even though the public has never been formally notified.i would move this higher

“It’s a kind of spatial-temporal mapping across doorways, hallways, common spaces, and adjacent walkways,” Kamran explained, “which enables nearly continuous tracking of individuals’ routines and associations.”

### ***Digital Access Meets Surveillance in NYCHA***



*(Photo by Paul Martinka)*

The New York City Housing Authority (NYCHA) houses, often recognized by their red-brick buildings and open courtyards, form one of the most visible parts of New York’s public housing system. Established in 1935, NYCHA was created to provide affordable housing for low- and moderate-income residents across the five boroughs. Today, more than 520,000 New Yorkers live in over 177,000 apartments within 335 developments.

These complexes often include shared spaces such as playgrounds, basketball courts, and community centers designed to support residents’ well-being. Despite their crucial role, NYCHA developments have faced long-standing challenges, including [a rate of violence and shootings](#) that, although it has decreased in recent years, remains disproportionately high relative to the population they represent.

In September 2022, to ensure that NYCHA residents could access [free, fast, and secure internet](#), the New York City Office of Technology and Innovation (OTI) officially launched Big Apple Connect, making deals with two service providers, Optimum and Spectrum.

Considered one of Mayor Bill de Blasio's signature initiatives, the official aim of this program was to close the [digital divide](#) in New York City. At first, it seemed like a major achievement. "[We just came out of COVID](#)," declared Talia Kamran, Staff Attorney in the Seizure and Surveillance Defense Project at Brooklyn Defender Services (BDS). "A lot of kids had to figure out how to learn remotely, and low-income kids weren't able to go to school, so this was going to be a huge and revolutionary development in public housing."

However, the digitization of the city's public housing infrastructure is now also being leveraged for enhanced surveillance of residents. There are already 68 video cameras sending live feeds to their local police precinct and, according to Anthony Mascia, Commanding Officer of the NYPD's Information Technology Bureau, the number of cameras across public housing is expected to increase to 1,900 by the end of the year.

It remains unclear how sites were selected, and no public data demonstrating the system's effectiveness has been released.

Despite this lack of transparency, Big Apple Connect, the program that links NYPD surveillance software to CCTV cameras in NYCHA developments, giving police real-time access to video feeds, will continue to expand.

### ***Public Safety or Racialized Surveillance?***



*Anthony Mascia, the commanding officer of the NYPD's Information Technology Bureau (right), and NYCHA Chief Operating Officer Eva Trimble testified at an emergency oversight hearing on police surveillance in NYCHA on September 30. | New York City Council*

On September 30, the City Council's Committees on Technology, Public Safety, and Public Housing held a joint oversight hearing, focusing on three main issues.

Council Members questioned whether, by deploying the system without further explanation, the Adams Administration was violating the Public Oversight of Surveillance Technology (POST Act), a law designed to increase transparency and oversight of the NYPD's use of new surveillance technologies and information-sharing networks.

In addition, several public defense organizations, including Brooklyn Defender Services (BDS) and [The Legal Aid Society](#), testified against the NYPD's plan to expand its CCTV surveillance across public housing complexes.

They argued that the initiative represents a violation of residents' *Fourth Amendment rights* - the amendment that protects Americans against unreasonable search and seizure - and results in disproportionate surveillance of Black and Latino communities, since residents of this housing are predominantly black and brown.

[The POST Act](#) was passed in 2020 to regulate NYPD surveillance policies and to require the department to publicly disclose information about the types of surveillance technologies it uses, including platforms such as the Domain Awareness System.

Since 2007, the department has spent billions of dollars on surveillance contracts, including New York's Domain Awareness System, a real-time surveillance map of the city procured from Microsoft for over \$1 billion, which unifies into a single centralized network more than a dozen public and private technologies, including camera

"It's a kind of spatial-temporal mapping across doorways, hallways, common spaces, and adjacent walkways," Kamran explained, "which enables nearly continuous tracking of individuals' routines and associations."

It was on the basis of these concerns that New York City Council Member Chris Banks posed a question to Anthony Mascia during the [public hearing](#) held on September 30:

"The Domain Awareness System is a counterterrorism tool. Is it standard practice for the NYPD to use surveillance technology in privately owned houses?" According to Kamran, this expansion appears to contradict several recent Supreme Court decisions.

In *Carpenter v. United States*, (2018), for example, the Supreme Court warned that 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. The Court held that the government's ability to chronicle a person's movements over time through cell-site location information (CSLI) constitutes a search under the Fourth Amendment because it "provides an

intimate window into a person's life, revealing not only his particular movements but through them his familiar, political, professional, religious, and sexual associations.”

This reasoning has become central to current debates over the NYPD's Domain Awareness System and related surveillance networks. As these technologies allow real-time tracking across public and semi-private spaces, integrating cameras, license-plate readers, and biometric tools, systems that could amount to the kind of “near perfect surveillance” that the Carpenter Court cautioned against.

In response to these objections, the NYPD stated that although the Domain Awareness System was originally designed as an anti-terrorism tool, its use in residential complexes is not intended for surveillance but rather to ensure the safety of residents, serving as a key resource in resolving potential criminal incidents. This point was reinforced by NYCHA Chief Operating Officer Eva Trimble, who defended the 2023 agreement for the installation of new cameras in NYCHA complexes. She emphasized that residents' privacy is protected since no one monitors the footage in real time, and that the push for increased surveillance and security actually comes from the residents and community representatives themselves.

Within this debate, surveillance raises questions about who is actually being surveilled. While the issue of public safety is undoubtedly an urgent concern for citizens, as Talia Kamran noted during her testimony, the more the NYPD concentrates its attention on communities of color, the more “evidence” it produces to justify even greater surveillance in those same neighborhoods. In other words, biased data produces biased results.

According to data from the [Resident Data Summary](#) published in 2024, the majority of people living in NYCHA housing - over 528,000 New Yorkers - identify as Black (44%) or Hispanic/Latino (42%).

As BDS Seizure and Surveillance Defense Project put it the latest reports “The majority of the people Brooklyn Defenders represents are people of color who live in neighborhoods subject to some of the heaviest policing and surveillance in the city. Our clients and their communities are monitored by street cameras, ShotSpotter, license plate readers, predictive policing systems, and NYPD databases. This CCTV program must also be understood within this historical context and the broader ecosystem of NYPD surveillance: we cannot trust that these cameras are being placed in a nondiscriminatory manner when the NYPD has a long-standing history of racial discrimination in policing, particularly in NYCHA developments.”

This harm is tangible, Kamran continued: “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.”

Referring to this fear, Kamran points to episodes that she said are frequently experienced by people living in neighborhoods such as the Bronx, Harlem, and Queens. Residents of low-income communities that experience higher crime rates often call for more public safety resources - a demand that has been used to justify increased surveillance investments: "They'll say, we want more police on our block".

On the other hand, she adds, "We constantly hear kids say, 'I hate walking to school because every day I get stopped by the NYPD and they ask me questions on my way there. I don't want to see them anymore, so I'm not going'."

### ***Gang Database, Transparency, and the Push for Digital Rights***



*(Photo by Frances Bruey for LDF)*

They are the same who, just because they live in some places, risk entering into the so-called [Gang Database](#): a secret Database which the NYPD created by designating thousands of New Yorkers as members of local street "crews."

According to the [Legal Defense Fund](#), whose mission centers on advancing racial justice, the NYPD operates its Gang Database with little to no due process protections. Individuals added to the list receive no official notification and are given no opportunity to contest the police

department's decision to label them as gang members. The data reveal a stark racial imbalance: ninety-nine percent of those identified as "gang" or "crew" members are Black and Latino boys and men.

This is the picture painted by the [latest report released on October 15](#) by the Office of the Inspector General for the NYPD (OIG-NYPD), part of the New York City Department of Investigation.

As Assembly member Emily Gallagher noted "the NYPD's Gang Database has become yet another mechanism through which the policing system perpetuates racial profiling against young Black and Latino men". She emphasized that inclusion in the database is not based on evidence of criminal activity but rather on arbitrary markers such as tattoos, clothing colors, or neighborhoods frequented.

Where the line between surveillance and security becomes blurred, transparency is essential to protecting citizens' rights, an idea that, however, seems to be lacking in both cases cited. The OIG-NYPD 2023 report highlighted serious transparency issues in the NYPD's gang database: many individuals are not notified of their inclusion, the criteria for entry and review are neither clear nor public, and internal access to the data is insufficiently regulated. This lack of transparency limits the right to know and challenge inclusion, reduces the accountability of the NYPD, and raises concerns about racial profiling of young Black and Latino individuals.

Similar concerns were raised during the September 30 hearing, where it emerged that NYCHA residents had not been informed about the connection between the Big Apple Connect program and the existing surveillance cameras.

On November 5, as celebrations for the election of New York's new mayor were winding down and social media feeds filled with profiles, behind-the-scenes insights, and election analysis, some of the city's leading digital rights organizations, including [Stop Surveillance](#) which fights to limit governmental surveillance and protect personal data, drew attention to a key point in the mayor's political agenda, which made the link between security and control a central element of his campaign.

One of the new administration's priorities will be the creation of a "Digital Sanctuary City", a political and technological proposal aimed at public safety. As emphasized by the newly elected mayor, the city must protect all residents, especially the most vulnerable, and surveillance programs based on discriminatory criteria do not effectively combat crime: "[citizens should not have to choose between safety and justice.](#)"