UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

PAMELA WRIDT AND ROBERT SAUVE, Plaintiffs, -against- CITY OF NEW YORK, Defendant.	No. _____ **COMPLAINT AND JURY DEMAND**

PRELIMINARY STATEMENT

1. You are being watched. Today, throughout New York City, the police are monitoring, tracking, and cataloging you. Nearly everywhere. Nearly all the time. Video cameras—body-worn, handheld, dashboard, stationary, and aerial—are recording you. License plate readers, location trackers, and gunshot detectors are tracking you. Your biometric data, including from DNA collection, and fingerprint and iris scanners is being stored. Phone taps, X-ray imaging, digital record aggregation, and financial analysis tools are gathering your electronic data. Your social media is being surveilled and scraped and your online posts stored; and social network analysis is being used to map out your relationships, religious beliefs, and political affiliations.

2. The mechanism that makes this surveillance possible is the City's Domain Awareness System, or the "DAS." It is a voyeuristic policing platform that unifies into one centralized network more than a dozen technologies—public and private—including video camera systems, tracking technologies, biometric tools, data and financial aggregation analytics, and digital communications monitors. Through the DAS, the New York City Police Department (the "NYPD" or the "department") collects the identity, location, banking details, vehicle information, social media activity, and friend groups of all who live in or enter the city. It

combines these entries with civil and criminal records and converts them into digital profiles that chart people's thoughts, plans, beliefs, and affiliations—reconstructing, in effect, the private lives of millions. It is virtually impossible to avoid.

3. The reach of this system is neither temporary nor limited. Information collected through the DAS is stored indefinitely, with no meaningful limits on its use by the department or the agencies with which it partners. Everyone—even those never suspected of any crime—is drawn into this web of surveillance, in open defiance of the constitutional limits that protect individual liberty and privacy. From the day it was launched, the DAS has subjected New Yorkers to suspicionless, city-wide surveillance that undermines their rights. It is an unprecedented violation of American life and now stands as one of the largest surveillance networks operated anywhere in the world.[1]

4. Despite its radical incursion into New Yorkers' privacy, the DAS has not met New York's public safety needs. New York has spent more than $3 billion amassing information that reveals the private lives of New Yorkers, including continued NYPD investment in discredited technologies. But the NYPD has failed to produce any conclusive evidence that this surveillance network has reduced crime. Despite all its invasiveness, the DAS has had no measurable impact on public safety.

5. Although the City has deliberately kept public information about the DAS scarce, the NYPD has revealed just enough to show that it is a digital surveillance powerhouse operating in plain sight. Those disclosures, trickled down in the press or buried in public hearings, combined with the visible presence of cameras, scanners, drones, and sensors send a chilling

[1] *Technology*, NYC.gov: New York City Police Department, About NYPD (last visited Sept. 21, 2025), https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/technology.page (noting that the DAS "utilizes the largest networks of cameras, license plate readers, and radiological sensors in the world").

message: New Yorkers are being watched. As a result, Plaintiffs and millions like them have been injured and intimidated, and their rights systematically chilled. Knowing that their movements and conversations may be captured, people inevitably change how they live. They block their windows to stop the cameras installed outside their homes from seeing inside. They change their commutes to avoid traffic scanners or abandon public transit altogether to keep their home and work addresses from being tracked. They censor their speech on social media and hesitate before joining public gatherings or community associations for fear of being recorded. The DAS traces what people do today, attaches it to a permanent file of their past, and—through algorithms—projects their future activities. Thus, New Yorkers have been put on notice that if they do not modulate their public behaviors, their actions may one day be used against them by their government.

6. Plaintiffs bring this action with reasonable cause to believe that they, like all who live in or visit New York City, have and will continue to be subjected to injury, intimidation, and interference in the exercise of their constitutional rights as long as the DAS remains in operation.

7. This civil rights action seeks to vindicate the fundamental protections of privacy, liberty, and speech guaranteed by the Constitution. Plaintiffs ask this Court to: (a) declare the City's surveillance practices unconstitutional intrusions on their rights; (b) provide relief to Pamela Wridt and Robert Sauve (collectively, "Plaintiffs") for the infringement of their rights; (c) enjoin Defendant from deploying the DAS against New Yorkers who are under no suspicion of criminal conduct; (d) require a warrant before the system may be searched for individuals' records; and (e) order the City to develop and enforce written policies governing the DAS, including the maintenance of an access log to prevent misuse or abuse, a data retention standard

mandating the deletion of all records after 90 days, and strict limits on the sharing of DAS data with outside agencies.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1343(a)(3)-(4) because Plaintiffs' claims arise under 42 U.S.C. § 1983, and seek redress of the deprivation, under color of state law, of rights guaranteed by the Constitution of the United States.

9. The instant action arises under the First and Fourth Amendments to the United States Constitution and 42 U.S.C. § 1983.

10. The acts complained of occurred in the Southern District of New York and venue is lodged in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events and/or omissions giving rise to the claims occurred in the District and Defendant resides in this district.

PARTIES

11. Plaintiff Pamela Wridt is a longtime resident of Brooklyn, New York, where she lives with her partner Plaintiff Robert Sauve. Together they have been subject to surveillance through the DAS in their shared Brooklyn home.

12. Plaintiff Robert Sauve is a native New Yorker and resident of Brooklyn, New York, where he lives with his partner Ms. Wridt. Together they have been subject to surveillance through the DAS in their shared Brooklyn home.

13. Defendant City of New York ("Defendant" or the "City") is and was at all relevant times a municipal entity created and authorized under the laws of the State of New York. It is authorized by law to maintain a police department, the NYPD, which acts as its agent

in law enforcement and for which it is ultimately responsible. The NYPD is a duly authorized public authority able to perform all functions of a police department under the applicable sections of the New York State Criminal Procedure Law. Defendant assumes the risks incidental to the maintenance of the NYPD's police force and the employment of police officers.

JURY DEMAND

14. Plaintiffs demand a trial by jury in this action.

FACTUAL BACKGROUND

15. The NYPD operates a massive, integrated surveillance platform known as the DAS.

The DAS Persistently Records New Yorkers' Movements

16. Created in 2008 and expanded in the years since,[2] the DAS consolidates under one platform a wide range of surveillance technologies that before could only exist separately. The DAS continuously collects, stores, and analyzes information about New Yorkers and visitors every day. It does so automatically, without individualized suspicion, without judicial authorization, and without human input.

17. The DAS brings together: (1) video cameras, including body-worn, handheld, dashboard, stationary, and aerial; (2) tracking tools, such as automated license plate readers ("ALPRs"), location trackers, and gunshot detectors; (3) biometric data, including from DNA collection, and fingerprint and iris scanners; (4) electronic monitoring devices, such as phone taps, X-ray imaging, digital record aggregation, and cryptocurrency analysis; and (5) social media surveillance, obtained by monitoring individuals' internet activity, scraping and storing

[2] E. S. Levine, Jessica Tisch, Anthony Tasso & Michael Joy, *The New York City Police Department's Domain Awareness System*, 47 INFORMS 70 (Jan. 18, 2017), http://dx.doi.org/10.1287/inte.2016.0860.

online posts, and using social network analysis to map out a person's relationships, religious beliefs, and political affiliations, among other things.[3]

18. By design, the DAS consolidates these distinct sources into a single, searchable application,[4] giving the NYPD the ability to track individuals across space and time.

19. The camera network alone is so extensive that it captures nearly every New Yorker as they go about daily life—commuting, going to church, visiting a doctor, attending a protest, or buying groceries.[5] And even when an individual is not recorded directly, the DAS infers their location through connected sensors and databases, linking it to biometric and identifying information. It delivers real-time, persistent tracking across the five boroughs.

20. One feature that distinguishes the DAS from traditional investigative methods, in addition to the massive scope of the data it collects, is its use of powerful analytics. Facial recognition software, correlation engines, and the use of artificial intelligence allow the NYPD to draw information at a scale unimaginable at the country's founding. Officers can, on information and belief, automatically track an individual across the city using computer vision software, which follows a person from one camera to the next based on descriptors as simple as the color of a piece of clothing. A process that once took days or weeks of manual review can now be done "with the snap of a finger," in the words of the Police Commissioner.

---

[3] INFORMS, *Presentation: The New York City Police Department's Domain Awareness System*, YouTube (Feb. 1, 2017) (timestamp 0:57), https://www.youtube.com/watch?v=dOwu4SMbVl4 (listing a non-exhaustive group of DAS technologies).

[4] NYPD, *Portable Electronic Devices: Impact and Use Policy*, NYC.GOV (Apr. 11, 2023), https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/portable-electronic-devices-ped-nypd-impact-and-use-policy_4.11.23_final.pdf (describing that NYPD-issued smartphones contain a mobile version of DAS).

[5] Levine, *supra* note 2 (discussing the search capabilities and in-house algorithms powering the DAS).

21. This analytical power is not limited to cameras. ALPRs record the time and location of vehicles as they move through the city, compiling a detailed record of where drivers travel, how often, and at what times. Social media monitoring software scrapes and analyzes online posts, revealing networks of friends and associates. Other DAS databases index physical characteristics such as scars, tattoos, medical conditions, and even the way a person walks.

22. The DAS gathers even more granular data on Black, Hispanic, Muslim, and immigrant residents, communities, and neighborhoods. While the DAS surveils all New Yorkers, non-White residents are even more likely to be monitored because facial recognition cameras and gunshot detectors are disproportionately located in non-White neighborhoods.

23. Teenagers and young people of color are particularly vulnerable to heightened levels of DAS surveillance. NYPD social media monitoring analyzes and collects online activity from tens of thousands of young Black and Hispanic New Yorkers and funnels the data into a Criminal Group Database, known as the GANGS Database,[6] which is available to officers through the DAS. Young people may be entered into the database merely for living in certain neighborhoods, using a particular social media hashtag, or associating with certain classmates. The database is comprised almost exclusively of people of color, placing Black and Hispanic youth at constant risk of harassment, arrest, detention, and worse.

24. All of this culminates in a staggering repository of information on New Yorkers of every background, yet the City imposes no known limits on how long it is retained or how it may be used—whether today or in years to come. It includes at least five years of ALPR data,

---

[6] Press Release, NYC Dep't of Investigation, Release No. 16-2023, *DOI's Office of the Inspector General for the NYPD Issues Report Examining NYPD's Use and Operation of the Criminal Group Database* (Apr. 18, 2023), https://www.nyc.gov/assets/doi/reports/pdf/2023/16CGDRpt.Release04.18.2023.pdf (report stating that all 33,763 uniformed NYPD officers have access via the Enterprise Case Management System's DAS search function to the GANGS Database, searchable by name).

thirty days of closed-circuit television footage or CCTV,[7] records from gunshot detection microphones, millions of 911 calls and 311 civilian complaints, arrest reports, parole and probation files, and state criminal records.[8] Additional databases maintained by other City agencies or private companies are also made available to the NYPD and folded into the DAS without limit.[9]

25. Each of the NYPD's approximately 36,000 uniformed officers have access to the DAS.

26. NYPD officers have access to the DAS through their workstations.[10]

27. NYPD officers have access to the DAS on their mobile phones.[11]

28. With a few taps, an officer can retrieve years of location data, view live camera feeds, pull arrest or complaint histories, and survey a person's social or political associations. This access is not limited to investigators or specialized units; it is distributed department-wide, without meaningful restrictions on scope or purpose. In practice, the application transforms every patrol officer into a mobile intelligence unit, capable of conducting warrantless surveillance at

---

[7] NYPD, *Domain Awareness System (DAS): Impact and Use Policy*, NYC.GOV (Apr. 11, 2021), https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/domain-awareness-system-das-nypd-impact-and-use-policy_4.9.21_final.pdf (detailing that "the NYPD utilizes Closed Circuit Television (CCTV) cameras throughout the five (5) boroughs … DAS behaves as a centralized repository through which authorized users can access CCTV cameras … NYPD Detectives, Sergeants, and higher ranked members can use DAS to view live feed from CCTV cameras").

[8] *Id.* (generally describing the capabilities of the DAS); *see also* Levine, *supra* note 2.

[9] *City Council, Committee on Public Safety: NYPD Data Purchasing Practices from Private Companies*, CITY MEETINGS NYC (Feb. 19, 2025), https://citymeetings.nyc/meetings/new-york-city-council/2025-02-19-1000-am-committee-on-public-safety/chapter/nypds-data-purchasing-practices-from-private-companies/.

[10] *Domain Awareness System (DAS): Impact and Use Policy*, *supra* note ("DAS efficiently centralizes vital information that would otherwise be kept throughout different isolated data compartments within NYPD computer systems.").

[11] *Portable Electronic Devices: Impact and Use Policy*, *supra* note 4 ("NYPD-issued PEDs contain a mobile version of the Domain Awareness System (DAS).").

will. The ease and range of access magnify the risks of misuse, removing natural barriers that once constrained surveillance and enabling the constant monitoring of New Yorkers.

29. Reports suggest that the DAS is commonly used in investigations,[12] yet there is no record of any officer ever being disciplined for unauthorized access. Nor is there evidence of a binding policy designed to restrict or monitor its use.[13] With no oversight, officers enjoy broad discretion to search the DAS for purposes that may be departmental as well as personal.

30. The NYPD has justified the DAS by pointing to crime prevention.[14] But years of evidence show that surveillance on this scale has not reduced crime.[15] And the department has conceded that some of its most expansive programs did not produce any credible leads. For all its reach into the lives of New Yorkers, the DAS offers intrusion without benefit.

The Aggregation of Technologies Within the DAS Reveals Constitutionally Protected Activity Unknowable from Any One Source

31. Many DAS components—facial recognition, ALPRs, social media monitoring—would raise serious constitutional concerns if used in isolation. In combination, however, they

---

[12] Mayor Eric Adams repeatedly affirms the DAS's centrality to the department's daily police work, and he appointed Police Commissioner Jessica Tisch based in large part on her leadership in developing the DAS. Press Release, New York City Press Office, *Mayor Adams Appoints Jessica Tisch as NYPD Commissioner*, NYC Office of the Mayor (Nov. 20, 2024), https://www.nyc.gov/office-of-the-mayor/news/847-24/mayor-adams-appoints-jessica-tisch-nypd-commissioner#/0.

[13] NYC Comptroller, *Audit Report on the Information System Controls of the Domain Awareness System Administered by the New York City Police Department*, OFFICE OF THE NYC COMPTROLLER (June 26, 2015), https://comptroller.nyc.gov/reports/audit-report-on-the-information-system-controls-of-the-domain-awareness-system-administered-by-the-new-york-city-police-department/ (finding that the NYPD had "no adequate standard criteria to review DAS user activities" and further noting that "we found that there were individuals who were no longer NYPD employees whose DAS access had not been deactivated in the system").

[14] Levine, *supra* note 2. (quoting former Police Commissioner William J. Bratton saying, "the DAS is essential in keeping New York City safe from crime and terrorism").

[15] *Historical New York City Crime Data*, NYC.gov: New York City Police Department, NYPD Stats (last visited Sept. 22, 2025), https://www.nyc.gov/site/nypd/stats/crime-statistics/historical.page (showing an increase in city-wide felonies since 2012).

produce an intolerably invasive system. Aggregated data enables the NYPD to uncover constitutionally protected activity such as political expression, religious practice, or private association, that would be unknowable from any single source. This aggregation magnifies the constitutional injury, creating violations far greater than the sum of the parts.

32. The unprecedented reach of the DAS is best understood by examining the categories of information it collects and fuses together.

33. ***First***, the system integrates various networks of cameras (*i.e.*, body cameras worn by police officers, handheld and dashboard cameras used in the field, stationary cameras fixed to poles and buildings, and aerial cameras mounted on drones or helicopters).

34. ***Second***, the DAS incorporates tracking technologies, such as ALPRs, location sensors, and gunshot detectors that record the presence and movement of people and vehicles throughout the city.

35. ***Third***, the NYPD adds biometric identifiers, including DNA samples, fingerprints, and iris scans, to match surveillance records to named individuals.

36. ***Fourth***, the DAS uses electronic monitoring systems that include phone taps capable of intercepting calls, X-ray imaging devices that scan vehicles and containers, programs that aggregate digital records from multiple databases, and software that tracks financial transactions.

37. ***Fifth***, the DAS collects information from the internet. It monitors online activity, gathers and stores posts from social media platforms, and uses software to study how people are connected to one another online. These tools give the NYPD access to records of what people say and share online, as well as the friends and associations they maintain. In the paragraphs that

follow, Plaintiffs describe how the Defendant operationalizes each of these categories, and how their combined use forms a surveillance apparatus far more invasive than each tool on its own.

Video Camera Technologies

38. The DAS camera network, as explained, combines footage from many different types of cameras. These include body-worn cameras carried by officers, handheld cameras used in the field, dashboard cameras mounted in police vehicles, stationary cameras fixed to poles and buildings, and aerial cameras attached to drones and helicopters.

39. The NYPD operates tens of thousands of stationary cameras across the city. These devices can pan, tilt and zoom, and capture both wide areas and fine details in high resolution. In most neighborhoods, camera coverage is so dense that residents cannot travel to work, school, or places of worship without being recorded.

40. The DAS further incorporates footage from tens of thousands of privately operated cameras. These include cameras maintained by businesses and other public and private institutions.[16] Unlike NYPD-owned cameras, which must be labeled, these private devices provide no public notice of their connection to the system. The department has not disclosed the full number of privately owned cameras integrated into the DAS.

41. In addition, cameras operated by other City agencies have been connected to the DAS. For example, the New York City Housing Authority ("NYCHA") operates more than 20,000 cameras. At least one NYCHA complex has already been integrated, with additional complexes scheduled to follow.

[16] *Domain Awareness System (DAS): Impact and Use Policy*, *supra* note 7 (describing "external stakeholders providing NYPD with access to their public-space facing cameras").

42. Aerial cameras expand the system further. Video captured by drones and helicopters is added into the DAS, allowing the department to monitor activity from above across entire blocks and neighborhoods.

43. Since 2018, the NYPD has deployed drones with growing frequency at public celebrations, social gatherings, and protests.[17] These drones capture high-resolution video, use thermal sensors, and record audio.[18] By 2024, the City had authorized the use of autonomous drones in response to 911 calls, gunshot alerts, and "crimes in progress as needed,"[19] with further expansions announced for 2025.[20]

44. Through the DAS interface, officers can view both archived recordings and live camera feeds. The system provides access to at least thirty days of stored footage, along with the ability to observe events as they unfold in real time.[21]

---

[17] *UAS (Drones) Reports & Analysis*, NYC.gov: NYC.gov: New York City Police Department, NYPD Stats (last visited Sept. 22, 2025), https://www.nyc.gov/site/nypd/stats/reports-analysis/uas-drones.page.

[18] Press Release, New York City Press Office, *Mayor Adams, Interim Police Commissioner Donlon Announce "Drone as First Responder" Program to Reduce Response Times and Keep New Yorkers Safe*, NYC Mayor's Office (Nov. 13, 2024), https://www.nyc.gov/office-of-the-mayor/news/827-24/mayor-adams-interim-police-commissioner-donlon-drone-first-responder-program-to#/0.

[19] Press Release, New York City Press Office, *Mayor Adams Announces New Drone Operations Committee*, NYC Mayor's Office (Jul. 22, 2025), https://www.nyc.gov/mayors-office/news/2025/07/mayor-adams-announces-new-drone-operations-committee.

[20] Press Release, New York City Press Office, *supra* note 18.

[21] NYPD, *Closed-Circuit Television (CCTV) Systems: Impact Use and Policy*, NYC.GOV (Oct. 26, 2023), https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/cctv-systems-nypd-Impact-and-use-policy_10.26.23.pdf.

45. NYPD officers also use camera feeds in the DAS to conduct facial recognition searches.[22] This allows comparison of an individual's face against recordings pulled from tens of thousands of feeds. Public reporting indicates that in recent years such searches have numbered in the tens of thousands annually.

46. All of these camera feeds—whether owned by the NYPD, contributed by private businesses, operated by other City agencies, or captured from the air—are accessible through the DAS without scrutiny.

Tracking Technologies

47. The DAS also integrates a wide array of tracking technologies, including ALPRs, location sensors, and gunshot detection systems. These devices record the presence and movement of people and vehicles across New York City and feed that information directly into the centralized DAS platform.

48. ALPRs form the backbone of this tracking network. These devices photograph and record vehicles as they pass unmarked checkpoints throughout the city, including every entry point to the island of Manhattan. Each record includes the vehicle's license plate number, location, and time, as well as the make, model, and color of the vehicle. In many cases, the devices also capture images of drivers and passengers, including children.

49. The most recent public disclosure of the NYPD's ALPR program occurred in 2014, when the department testified before the City Council that it operated approximately 500

[22] *Domain Awareness System (DAS): Impact and Use Policy*, *supra* note 7 (describing DAS capabilities generally; specifying that still images the DAS collects "may be used as a probe image for facial recognition analysis").

such devices.[23] Since then, the program has expanded considerably. ALPR data is combined with other surveillance information in the DAS, allowing officers to reconstruct detailed records of individuals' routines and relationships.

50. ALPR data is further supplemented by records obtained from private companies and out-of-state law enforcement partners. In 2015, the NYPD contracted with Vigilant Solutions, Inc., now a subsidiary of Motorola, to access its nationwide database of more than two billion license plate records. Vigilant Solutions adds over one million new records each day. Through Vigilant's platform, NYPD officers can use functions such as "stakeout," which identifies likely locations to find a vehicle based on past patterns; "associate analysis," which flags vehicles commonly seen together; and "predictive analysis," which attempts to forecast a person's future location based on past travel routines. The NYPD holds on to the license plate data for at least five years regardless of whether a car triggers any suspicion.[24]

51. The DAS also incorporates other tracking devices. Location sensors are deployed to record patterns of movement across the city, while gunshot detection systems log and transmit the location of possible shootings in real time. These data streams are integrated alongside ALPR data to expand the department's ability to record movements and relate them to individuals.

52. Since 2015, the NYPD has invested in ShotSpotter, a gunshot detection system that relies on acoustic sensors to classify loud noises as potential gunfire.[25] These sensors operate

---

[23] John J. Miller, Deputy Comm'r of Intelligence & Counterterrorism, N.Y.C. Police Dep't, *Testimony Before the N.Y.C. Council Committees on Public Safety and Fire and Criminal Justice Services*, NYCLU (Nov. 12, 2014), https://assets.nyclu.org/DC_Miller_Testimony.pdf.

[24] NYPD, *License Plate Readers: Impact and Use Policy*, NYC.GOV (Apr. 11, 2021), https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/license-plate-readers-lpr-nypd-impact-and-use-policy_4.9.21_final.pdf.

[25] *See also* NYPD, *ShotSpotter: Impact and Use Policy*, NYC.GOV (Apr. 11, 2021), https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/shotspotter-nypd-impact-and-use-

continuously, twenty-four hours a day, and are sensitive enough to record conversations of people nearby, sometimes even inside their homes.[26] When triggered, ShotSpotter triangulates a location and alerts officers through the DAS.[27] According to City records, Defendant has spent more than $45 million to install and maintain these microphones, which now cover wide areas of the city.[28] ShotSpotter data—including audio clips, timestamps, and location information—is stored within the DAS.[29]

53. ShotSpotter's accuracy has been repeatedly questioned. The City Comptroller reported that up to 84 percent of alerts may be false alarms, and more than 99 percent of responses fail to recover a firearm or identify a suspect.[30] Other jurisdictions, including Chicago and Seattle, have abandoned ShotSpotter because of these shortcomings. Yet the NYPD continues to invest in the technology, adding vast streams of sensitive audio to the DAS, even as its efficacy in reducing crime remains unproven.

---

policy_4.9.21_final.pdf (describing NYPD's gunfire-detection acoustic sensors, access to confirmed gunfire event data via the DAS, limitations on sensor audio capture, data retention, and roles of authorized users).

[26] *Id.*

[27] *Domain Awareness System (DAS): Impact and Use Policy*, *supra* note 7 (describing that ShotSpotter is integrated into the DAS so that when a gunshot detection microphone captures a sound event, the confirmed gunfire alert data is relayed into the DAS for use by authorized users).

[28] NYC Comptroller, *Audit Report on the New York City Police Department's Oversight of Its Agreement with ShotSpotter Inc. for the Gunshot Detection and Location System*, OFFICE OF THE NYC COMPTROLLER (June 20, 2024), https://comptroller.nyc.gov/reports/audit-report-on-the-new-york-city-police-departments-oversight-of-its-agreement-with-shotspotter-inc-for-the-gunshot-detection-and-location-system/ (reporting that NYPD had spent $45.4 million on ShotSpotter from August 14, 2014 through June 30, 2023).

[29] *ShotSpotter: Impact and Use Policy*, *supra* note 25.

[30] NYC Comptroller, *supra* note 28 (finding that NYPD responded to thousands of ShotSpotter alerts, but only 8-20% of alerts sampled during 2022-2023 were confirmed as shootings; NYPD spent over 426.9 hours in June 2023 alone investigating alerts that did not result in confirmed shootings).

Biometric Technologies

54. The DAS incorporates biometric identifiers that tie surveillance data directly to individuals. These include DNA samples collected by the NYPD, fingerprint records drawn from both criminal and civil sources, and iris scans.

55. The NYPD—in partner with the Office of the Chief Medical Examiner—maintains one of the largest DNA databases in the country, with more than 100,000 profiles, many collected from individuals never convicted of a crime. These records are integrated into the DAS, allowing officers to link genetic material to other surveillance entries.

56. In addition, fingerprint databases maintained by the Office of Criminal Justice and the NYPD are accessible through the system. These records connect individuals to arrests, summonses, and other official contacts.

57. The department has also introduced iris scanning used as part of its identification practices.[31] Iris scans, like fingerprints and DNA, provide a permanent and unique marker of identity, and their integration into the DAS allows for cross-referencing against other surveillance streams.

58. Some biometric records enter the DAS not through criminal investigations but through everyday dealings with City agencies—for example, when residents apply for services, permits, or benefits.[32]

---

[31] NYPD, *Iris Recognition: Impact and Use Policy*, NYC.GOV (Apr. 11, 2021), https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/iris-recognition-nypd-impact-and-use-policy_4.9.21_final.pdf.

[32] *E.g.*, Driver's license photos collected for everyday identification purposes are accessible to law-enforcement facial-recognition searches without notice to the individuals involved, and New York agencies have shared DMV records with NYPD for investigations. NYPD also describes the DAS as a central hub that aggregates multiple databases and allows officers to extract images for facial-recognition comparison. *See* Levine, *supra* note 2 (describing the DAS as a network of "sensors, databases, devices, software, and infrastructure that delivers tailored information and analytics to mobile devices and precinct desktops").

59. Individuals are not informed that this information may be added into a policing database.

60. In this way, data collected for ordinary civic purposes is converted into a tool of criminal surveillance, even for those never suspected of wrongdoing.

Electronic Monitoring Technologies

61. The NYPD employs electronic monitoring through the DAS using tools such as phone taps that intercept and record calls; X-ray imaging devices that scan vehicles, packages, and containers; programs that pull together digital records from multiple City and law enforcement databases; and software that traces transactions across financial networks.

62. Through the DAS, the department can intercept and record phone calls. These recordings are not limited to the fact that a call occurred; they can capture the content of conversations and the identities of those on the line. This allows the NYPD to move well beyond identifying the fact of a call and into the content, context, and associations that the call reveals.

63. X-ray imaging devices add another layer of monitoring. These scanners, deployed at bridges, tunnels, and other checkpoints, can penetrate vehicles and cargo containers to reveal their contents without physical entry.[33] Data from these scans, when integrated into the DAS, provides the NYPD with a rolling catalog of private property and movements that would otherwise be beyond government scrutiny.[34]

---

[33] NYPD, *Mobile X-Ray Technology: Impact and Use Policy*, NYC.GOV (Apr. 11, 2021), https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/mobile-x-ray-technology-nypd-impact-and-use-policy_4.9.21_final.pdf.

[34] *Id.*

64. Digital record aggregation further broadens the reach of the DAS. Programs pull together information from multiple databases maintained by City agencies and law enforcement partners, ranging from administrative records to enforcement histories.[35]

65. The DAS also incorporates financial and cryptocurrency analysis software. According to NYPD disclosures, the department has invested in banking and blockchain forensics tools that allow investigators to trace money across centralized and decentralized networks.[36] With these tools, the department can examine public banking and blockchain records (as well as internet payment platforms like PayPal, Venmo, and Cash App) for information tied to financial transactions, follow the movements of funds, and identify the individuals tied to that banking activity.[37]

Social Media Surveillance

66. Finally, the DAS surveils the online activities and speech of New Yorkers. The system collects and stores information from social media platforms, including Facebook, Instagram, Twitter, and TikTok. Posts, photographs, and messages are scraped in bulk, together with identifying details (*e.g.*, timestamps, geolocation tags, and network connections) about the individuals that publish them.

67. NYPD officers also employ undercover methods online. Officers create and operate fake social media accounts to impersonate peers, join messaging groups, and interact with individuals for the purpose of gathering intelligence.

---

35 *Domain Awareness System (DAS): Impact and Use Policy*, *supra* n.7.

36 NYPD, *Cryptocurrency Analysis Tools: Impact and Use Policy*, NYC.GOV (Apr. 11, 2021), https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/cryptocurrency-analysis-tools-nypd-Impact-and-use-policy_4.9.21_final.pdf.

37 *Id.*

68. Information gathered through these methods is integrated into the broader DAS. A photograph shared online may be matched with a facial recognition hit from a surveillance camera; a post about attending a gathering may be linked to license plate reader data showing travel to that location. In this way, online activity is fused with physical tracking systems to create a more comprehensive record of a person's life.

69. To manage this enormous volume of data, the NYPD relies on analytics tools that employ machine learning and artificial intelligence.[38] These tools are used to detect patterns and to track individuals across the many different data streams captured in the DAS.[39] Automated systems scan millions of entries for specified individuals, objects, or behaviors. One example mentioned above is that a person can be followed across multiple videos based on something as simple as the color of their clothing. Patternizr, another DAS tool, processes thousands of reports to identify purported similarities among alleged crimes—connections that no officer could manually detect.

70. Through this integration of technologies and advanced analytics, the DAS turns New Yorkers' lives into permanent, searchable dossiers. Their movements can be reconstructed, cross-referenced with other datasets, and used to monitor activity that is constitutionally protected. And because the City has imposed no restrictions on either the duration or the use of the DAS, every New Yorker must live with the uncertainty of not knowing when, how, or by whom their lives will be probed. Nor can they know what new technologies will emerge to boost this surveillance in the years ahead.

---

[38] *Compare Domain Awareness System (DAS): Impact & Use Policy*, *supra* n.7, at 10 (stating that the DAS "does not use video analytics") *with* Levine, *supra* n.2 (stating that the DAS deploys automated pattern recognition, machine learning, and data visualization, and that analytic methods are "built into the DAS software").

[39] *Id.*

The NYPD Uses the DAS to Share New Yorkers' Data with Local, State, and Federal Agencies

71. The NYPD shares the personal information of New Yorkers collected through the DAS with outside entities. Data drawn from cameras, ALPRs, biometric identifiers, social media, and other sources is shared with other City agencies, State law enforcement, and the federal government. This sharing occurs without notice to the individuals whose data is involved and without their consent.

72. One way the department shares information from the DAS is through its participation in joint task forces. NYPD officers regularly work alongside local agencies and federal partners, including investigators from the Department of Homeland Security (DHS).[40] In these settings, officers can bring DAS data into the investigation and transmit it to their counterparts. Once that information enters federal control, the NYPD has acknowledged that it loses control over how the recipients may use it.[41]

73. ALPR databases aggregated by NYPD likewise appear vulnerable to federal access. Recent disclosures have revealed that ALPR data has been shared in joint investigations

---

[40] *See, e.g.,* Press Release, NYC Press Office, *Mayor Adams on Homeland Security Operation NYC Last Night*, NYC Office of the Mayor (Jan. 28, 2025), https://www.nyc.gov/mayors-office/news/2025/01/mayor-adams-on-homeland-security-operation-nyc-last-night?utm; Robert Griffin, *Working with NYPD and First-Responder Partners to Keep Our Cities Safe*, U.S. DEP'T. OF HOMELAND SECURITY (Nov. 24, 2015), https://www.dhs.gov/archive/news/2015/11/24/working-nypd-and-first-responder-partners-keep-our-cities-safe?utm; Press Release, DHS S&T, *S&T Works with NYPD to Test Communication Systems*, U.S. DEP'T. OF HOMELAND SECURITY (Aug. 1, 2017), https://www.dhs.gov/archive/science-and-technology/news/2017/08/01/st-works-nypd-test-communication-systems?utm.

[41] *See City Council, Committee on Public Safety: Information Sharing Between NYPD and Federal Law Enforcement Partners*, CITY MEETINGS NYC (Feb. 19, 2025), https://citymeetings.nyc/meetings/new-york-city-council/2025-02-19-1000-am-committee-on-public-safety/chapter/information-sharing-between-nypd-and-federal-law-enforcement-partners/ (Gerber testimony, 1:29:50–1:30:22) (stating that "if we're working on a joint investigation [with federal or state partners], typically we part . . . as part of a task force, we're gonna[sic] share whatever is relevant to that criminal investigation," and that the department in effect "loses control" over how shared data may be used).

with other law enforcement agents. By the NYPD's own account,[42] these records move across state lines, placing New Yorkers under surveillance by agencies far removed from this jurisdiction.

74. Public oversight and City Council hearings have raised concerns that those external uses may include civil immigration enforcement or political surveillance, despite City law prohibiting the use of local resources for such purposes.[43] Those concerns were confirmed in May 2025, when reports revealed that the NYPD transmitted personal information about a protester—including a sealed arrest record—to U.S. Immigration and Customs Enforcement. The department later admitted to the disclosure. That episode shows how New Yorkers' personal data, once captured by the DAS, can escape protections under local law and be used for purposes wholly unrelated to its original collection.

75. The department's partnerships with private entities expand this information flow still further. Programs such as NYPD SHIELD[44] and the Lower Manhattan Security Initiative[45]

---

[42] *City Council, Committee on Public Safety: Control over NYPD Data Once Shared with Task Forces*, CITY MEETINGS NYC (Feb. 19, 2025), https://citymeetings.nyc/meetings/new-york-city-council/2025-02-19-1000-am-committee-on-public-safety/chapter/control-over-nypd-data-once-shared-with-task-forces/ (statement of Deputy Comm'r Gerber at 1:34:41–1:34:50) ("we cannot dictate to federal agencies what they can or can't do as part of their federal investigations," acknowledging that once data is shared with a task force, the NYPD "cannot control how task forces or other entities use the shared data" and whether they decide to pass the data to "other entities").

[43] *City Council, Committee on Public Safety: NYPD's Data Sharing Practices With Other Law Enforcement Agencies*, CITY MEETINGS NYC (Feb. 19, 2025), https://citymeetings.nyc/meetings/new-york-city-council/2025-02-19-1000-am-committee-on-public-safety/chapter/nypds-data-sharing-practices-with-other-law-enforcement-agencies/ (testimony of Deputy Commissioner Michael Gerber) (describing NYPD's information-sharing with ICE, FBI, and other federal and local agencies).

[44] NYPD SHIELD, *About*, https://www.nypdshield.org/about/ (last visited Sept. 25, 2025) (describing NYPD SHIELD as a public–private partnership through which the department collaborates with private sector security personnel, emphasizing a "two-way street" of information flow in which the department shares intelligence and alerts while private sector participants provide situational reporting).

[45] NYPD, *Counterterrorism Bureau*, NYC.GOV (last visited Sept. 25, 2025), https://www.nyc.gov/site/nypd/bureaus/investigative/counterterrorism.page; NYPD SHIELD, *Lower Manhattan*

were designed to collect data from private-sector feeds. These same channels allow outward sharing of information, meaning data first aggregated into the DAS can ultimately move into the hands of non-NYPD recipients, including private parties.

76. These practices develop amidst a broader federal effort to consolidate and exploit Americans' personal data. Under the Department of Government Efficiency ("DOGE") and in partnership with private contractors such as Palantir, the federal government has begun combining records from various agencies like the Internal Revenue Service, the Social Security Administration, and the Department of Veterans Affairs. This trend has profound consequences for New Yorkers. Once the NYPD transmits DAS surveillance to federal partners, it can be combined with these other federal repositories and repurposed for prosecutions far beyond the borders of New York. Already, doctors in the city have been threatened with out-of-state prosecutions for providing reproductive care that is legal in this State but criminalized elsewhere. The NYPD's decision to share its residents' personal information with federal authorities exposes New Yorkers to precisely these harms.

77. The DAS operates not only as a local surveillance platform but as a conduit to larger systems of national intelligence and law enforcement. Once data leaves the NYPD's hands, there is no practical means of knowing where it travels, how long it is retained, or how it may be used. For New Yorkers, information first captured on a city street can resurface in the files of federal officers, distant prosecutors, or agencies with no connection to the community where it was collected.

Security Initiative (describing establishment of a network of 3,000 public and private surveillance cameras to monitor vehicles and pedestrians); *NYCLU v. New York City Police Department (Seeking access to information on Lower Manhattan Security Initiative under FOIL)*, NYCLU (Sep. 17, 2008), https://www.nyclu.org/court-cases/nyclu-v-new-york-city-police-department-seeking-access-information-lower-manhattan-security (last visited Sept. 25, 2025) (litigation seeking disclosure of records concerning the scope of the Initiative).

By Operating the DAS, the City Violates the Rights of New Yorkers, Including Plaintiffs

78. The existence and operation of the DAS is changing how New Yorkers live their lives. When people's locations, associations, and activities are continuously tracked, they change their behaviors. Some may choose different routes to work or school to avoid dense clusters of cameras. Others may alter the times they travel or even forego public transportation to limit exposure to license plate readers or surveillance in the subway system. Like the Plaintiffs here, New Yorkers begin to live not with freedom of movement, but with the calculation of how to avoid being watched.

79. As a result, the DAS is forcing New Yorkers to rethink how they interact with one another. People who once gathered freely with family, friends, and colleagues in public—whether at restaurants, parks, houses of worship, or community centers—now hesitate or change their plans, aware that their presence can be recorded, logged, and preserved.

80. One example is the impact on religious communities. Faith leaders have curtailed their activities out of fear of surveillance. Faith communities have reduced services, stepped back from public advocacy, or limited attendance at religious gatherings to avoid drawing the attention of law enforcement. Congregants, in turn, refrain from seeking counsel or participating fully in worship, chilled by the possibility that their presence could be recorded, retained, and used against them.

81. Artists, writers, students, workers, and advocacy organizations have also expressed hesitation to gather in groups or engage in public expression. They worry about being targeted, watched, or labeled by association. This has undermined their work and diminished the vibrancy of public life, curtailing the very freedoms of expression, speech, and association that New York City has long prided itself on protecting.

82. The same fear deters New Yorkers from seeking critical medical care, social services, or community support. People who need to visit health clinics, counseling centers, shelters, or legal aid offices may hesitate, aware that their presence at such locations could be tracked and retained by the DAS. Others avoid approaching service providers altogether, fearing that their private needs could become known to third parties or used against them.

83. The result is a climate of fear and self-censorship. New Yorkers are altering their conduct and constraining their associations to avoid the gaze of the DAS. Plaintiffs in this case have experienced this chilling effect firsthand.

Pamela Wridt and Robert Sauve

84. Plaintiffs Pamela Wridt and Robert Sauve are longtime residents of Brooklyn, New York. They share their home in Brooklyn, where they live together in the Bedford-Stuyvesant neighborhood. They are first-time homeowners, deeply rooted in their community, and engaged in civic, academic, and advocacy work.

85. Ms. Wridt is a children's rights advocate and researcher. She has also engaged directly with the department regarding surveillance in her own neighborhood, including filing a civilian complaint and records request concerning the two NYPD-owned cameras installed outside her residence.

86. Mr. Sauve is a professional radio disc jockey. He has been subjected to police surveillance and harassment since adolescence, beginning with stop-and-frisk encounters. Over the years, he has been photographed by NYPD officers at protests and has faced persistent monitoring in his neighborhood.

87. Both Mr. Sauve and Ms. Wridt live under the constant gaze of DAS surveillance as the NYPD mounted a box with two cameras directly outside their home, aimed at their living

room and bedroom windows. The cameras' presence has transformed what should be their place of safety into a space of anxiety. They have covered their windows with foil to block the cameras' view, depriving themselves of sunlight and the simple enjoyment of looking outside. Ms. Wridt describes the omnipresent surveillance as a daily violation, one that has left her unable to feel at ease in her own home.

88. Mr. Sauve and Ms. Wridt have also lost the enjoyment and value of their home. Because of the constant surveillance, they no longer use their front yard, rent out their apartment unit, open their blinds, or open their windows widely for air. The presence of the cameras has diminished their property's worth and inflicted ongoing emotional distress. For Mr. Sauve, who suffers from a chronic illness aggravated by stress, the constant surveillance has had serious health implications.

89. The DAS cameras have also eroded Plaintiffs' sense of community. Neighbors have become divided over its presence, and what once was a block with a spirit of mutual trust now is fractured. Plaintiffs believe the device unfairly targets the Black and Brown children on their block, raising serious concerns for the wellbeing of their community.

90. Beyond their home, Mr. Sauve and Ms. Wridt continue to feel the reach of the DAS throughout the city. Ms. Wridt reports a pervasive awareness of cameras wherever she travels, whether by foot, rideshare, or subway. Mr. Sauve no longer attends protests, deterred by NYPD officers photographing participants. Both Mr. Sauve and Ms. Wridt believe their activism and associations have placed them under heightened scrutiny, chilling their ability to exercise their rights freely.

FIRST CAUSE OF ACTION
Fourth Amendment
(42 U.S.C. § 1983)

91. Plaintiffs repeat and reallege the above paragraphs as if the same were fully set forth at length herein.

92. 42 U.S.C. § 1983 prohibits any person acting under color of state law, custom, or usage to deprive a citizen of rights secured by the Constitution.

93. Defendant's widespread and persistent warrantless DAS surveillance violates the Fourth Amendment because it infringes upon a reasonable expectation of privacy in the whole of Plaintiffs' movements and captures information about the privacies of life.

94. First, this program results in indiscriminate searches of Plaintiffs lacking any individualized suspicion or judicial approval, which are prohibited by the Fourth Amendment, and no exception to the Fourth Amendment's warrant requirement applies.

95. Second, Defendant's use and analysis of information collected through the DAS absent judicial authorization also violates the Fourth Amendment.

96. And third, Defendant's procedures governing this surveillance are constitutionally unreasonable.

97. Defendant acted, pursuant to an official municipal policy, under pretense and color of state law, in abuse of powers and beyond the scope of Defendant's authority and jurisdiction to willfully, knowingly, and intentionally deprive Plaintiffs of their constitutional rights secured by 42 U.S.C. § 1983, and by the Fourth Amendment to the United States Constitution.

98. As a direct and proximate result of the misconduct and abuse of authority detailed above, Plaintiffs sustained the damages hereinbefore alleged.

SECOND CAUSE OF ACTION
First Amendment
(42 U.S.C. § 1983)

99. Plaintiffs repeat and reallege the above paragraphs as if the same were fully set forth at length herein.

100. 42 U.S.C. § 1983 prohibits any person acting under color of state law, custom, or usage to deprive a citizen of rights secured by the Constitution.

101. At all relevant times, Defendant acted under color of state law.

102. Under the First Amendment to the Constitution of the United States of America, Plaintiffs have the right to free association and free expression.

103. Defendant's warrantless DAS surveillance program violates the First Amendment because its constant and inescapable monitoring deters and prevents people, including Plaintiffs, from free association and free expression, infringing on that right.

104. As a direct and proximate result of Defendant's unlawful widespread, unconstitutional conduct, pursuant to official municipal policy, Plaintiffs have sustained the damages hereinbefore alleged.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request judgment against Defendant as follows:

a. Declaring that the policies, practices, and acts of Defendant with regard to the DAS described here are unlawful and violate the First and Fourth Amendments to the Constitution of the United States;

b. Enjoining Defendant, Defendant's agents, employees, and successors, and all other persons in active concert or participation with Defendant from DAS surveillance until remedial measures are developed and implemented to safeguard

the First and Fourth Amendment rights of those subjected to the scope of the DAS;

c. Ordering Defendant to expunge all records of Plaintiffs created and maintained as a result of the unconstitutional and unlawful practices described herein;

d. Ordering Defendant to foreclose and discontinue the operation of DAS cameras situated so as to monitor residential streets in a manner that captures the private spaces of residences, including Plaintiffs Mr. Sauve's and Ms. Wridt's home;

e. Ordering Defendant to delete all data stored in the DAS after 90 days;

f. Enjoining Defendant from accessing DAS data for the 90 days that it is stored absent a warrant;

g. Awarding such damages to Plaintiffs as will fully compensate them for their loss of rights and emotional distress suffered due to Defendant's unlawful conduct;

h. Awarding Plaintiffs reasonable attorneys' fees, costs, and expenses incurred in prosecuting this action; and

i. Granting all such other further relief as may be just and proper.

Dated: New York, New York
October 27, 2025

EMERY CELLI BRINCKERHOFF
ABADY WARD & MAAZEL LLP

By: _____
O. Andrew F. Wilson
Sara Luz Estela
One Rockefeller Plaza, 8th Floor
New York, New York 10020
(212) 763-5000

SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT, INC.
Albert F. Cahn
Anya Weinstock
Darío Maestro
40 Rector Street, 9th Floor
New York, New York 10006
(212) 518-7573

Attorneys for Plaintiffs