BRENNAN CENTER FOR JUSTICE

New York City Police Department Surveillance Technology

By Ángel Díaz PUBLISHED OCTOBER 7, 2019

In every age, police forces gain access to new tools and technologies that may advance their mission to prevent and combat crime. The deployment of new technologies requires an understanding of their impacts on the fundamental rights of the communities that police serve and the development of safeguards to prevent abuse. The New York Police Department (NYPD), however, has purchased and used new surveillance technologies while attempting to keep the public and the City Council in the dark.

This chart provides an overview of the NYPD's surveillance technology, based on publicly available information, as well as the potential impact of the use of these tools. Because the police insist on complete secrecy, however, the picture is far from complete. The NYPD should not be allowed to prevent the public and its elected representatives from learning basic information necessary on these technologies, which is critical to effective oversight and the establishment of safeguards to protect the privacy and civil liberties of New Yorkers. The POST Act, introduced by Council Member Vanessa Gibson and currently supported by 28 co-sponsors, would require NYPD to take these steps.

Facial Recognition

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
Facial recognition systems attempt to identify or verify the identity of individuals based on their face. Different systems analyze face characteristics in photos or video feeds, or through real-time surveillance.	Facial recognition raises the following concerns: **Race, Gender, and Age Bias.** Numerous studies have found that facial recognition performs poorly when analyzing the faces of women, children, and people with darker skin tones.[1] This places communities already subject to over-policing at greater risk of misidentification. **Privacy.** Facial recognition is recognized as extraordinarily intrusive, challenging reasonable expectations of privacy and lacking necessary oversight. This is why a number of groups have called for a moratorium on facial recognition. **Free Speech.** Law enforcement use of facial recognition can chill the exercise of First Amendment rights by exposing protesters to persistent surveillance and identification. **Regulation.** There have been widespread calls for its regulation[2], and some cities — such as San Francisco[3]; Oakland[4], CA; and Somerville, MA[5] — have even banned its use.	Chief of Detectives Memo #3 (2012). NYPD's Facial Identification Section (FIS) runs static photos obtained from various sources, including databases of arrest photos, juvenile arrest photos of children as young as 11, and photos connected to pistol permits, among others.[6] The system analyzes a photo against those databases and generates potential matches.[7] The system will return a list of 200+ potential matches from which an FIS investigator selects one.[8] Where the footage is blurry or otherwise unusable, the NYPD can use photo editing tools to replace facial features in a reference photo so it more closely resembles those in mugshots.[9] The NYPD has also run photos of celebrities through its facial recognition system to try to identify suspects that resemble the celebrity where the original photo returned no matches.[10] The effectiveness of these techniques is doubtful.	Garbage In, Garbage Out – Face Recognition on Flawed Data (Georgetown Law Center on Privacy & Technology) The NYPD uses altered images in its facial recognition system, new documents show (The Verge) Review on the effects of age, gender, and race demographics on automatic face recognition (The Visual Computer, Volume 34) She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database (The New York Times) Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification (Proceedings of Machine Learning Research, Volume 81) NYPD ripped for abusing facial-recognition tool (NY Daily News) Coalition Letter Calling for a Federal Moratorium on Face Recognition (ACLU) Face it: Recognition technology isn't close to ready for prime-time (NY Daily News) Face it: This is risky tech. We need to put strong controls on face-recognition technology (NY Daily News) Facial Recognition Is Accurate, if You're a White Guy (The New York Times) Interactive Facial Recogntion Map (Fight for the Future)

Video Analytics

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
These systems analyze surveillance camera footage and attempt to isolate people and objects within the video feed. Video analytics use algorithms to spot particular articles of clothing and luggage. Certain versions claim they can find people in surveillance footage that match a particular hair color, facial hair, and even skin tone.	Video analytics raise the following concerns: **False Positives.** Information from video analytics can be incorrect and lead to unnecessary and potentially dangerous police encounters. **Free Speech.** Video analytics, like facial recognition, can chill First Amendment activity by exposing individuals to persistent surveillance as they move about the city. **Racial Bias**. Without adequate controls, targeting individuals based on their perceived ethnicity has the ability to exasperbate racial disparities in policing. **Privacy.** Video analytics allow for persistent surveillance as individuals move throughout the city, challenging traditional expectations of privacy.	No standalone NYPD policy is available, though video analytics may fall under the Public Security Privacy Guidelines that govern the NYPD's Domain Awareness System. These guidelines make no mention of video analytics, however, and they do not include standards governing the use or storage of analytics information. IBM developed object identification technology through a partnership with the police that gave the company access to the department's camera footage.[11] The NYPD then acquired IBM's object identification system to incorporate it into the NYPD's Domain Awareness System.[12] As of April 23, 2019, IBM stopped marketing certain versions of its Video Analytics program to additional cities.[13] It is not clear what this means for IBM's existing customers. According to the NYPD, the analytics system is intended to automatically alert NYPD officials to activities, such as "suspicious package was left" or "loitering."[14] A version of IBM's Intelligent Video Analytics 2.0, which allows users to search based on ethnicity tags, was allegedly tested but never incorporated into the NYPD's broader surveillance infrastructure.[15]	IBM Intelligent Video Analytics (IBM Vendor Material) IBM Presentation Regarding NYPD Video Analytics Development (IBM) IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color (The Intercept) The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy (ACLU)

Social Media Monitoring

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
Social media monitoring can be divided loosely into three categories: (1) Monitoring or tracking an individual, a group, or an affiliation (e.g., an online hashtag) via publicly available information; (2) Using an informant, a friend of the target, or an undercover account to obtain information from a protected or private account; or (3) Using software to monitor individuals, groups, associations, or locations. Police officers can also obtain warrants or use other legal processes to direct a social media platform to provide information, such as direct messages, metadata, and subscriber information.	Social media monitoring raises the following concerns: **False Positives.** What people say and do on social media are difficult to interpret, and connections on social media can be given undue importance or misunderstood completely. **Privacy.** Social media monitoring is intrusive, challenging individuals' reasonable expectations of privacy in online communications. **Racial Bias.** In the context of gang investigations, communities of color (especially children) are more likely to have their online activity surveilled. **Free Speech.** Surveilling social media also has the potential to chill free expression, including by causing individuals to self-censor and by monitoring lawful protest activities and other forms of protected association.	NYPD Detective Guide (2013) and Operations Order 34: Use Of Social Networks for Investigative Purposes – General Procedure, New York Police Department (2012). Policies permit officers to monitor social media for information and investigative leads. Handschu Guidelines (2017). These guidelines are the result of a settlement arising out of the NYPD's unconstitutional surveillance of protesters and religious minorities. The Handschu Guidelines allow officers to carry out general topical research, but they prohibit them from searching for individuals' names.[16] However, to develop intelligence information or to detect or prevent terrorism or other unlawful activities, the NYPD is also permitted to conduct online searches in the same manner as any member of the public, which would permit the police to access popular social media platforms.[17] Various NYPD units engage in social media monitoring, including the Intelligence, Juvenile Justice, Counterterrorism, Gang Enforcement, Internal Affairs, Executive Staff Identity Protection, and Threat Assessment divisions.[18] The full extent of social media monitoring by the NYPD is unknown, but it has been used in investigations ranging from tracking alleged gang activity[19] to surveilling Black Lives Matter protesters.[20]	Government Monitoring of Social Media: Legal and Policy Challenges (Brennan Center) NYPD monitoring of Black Lives Matter protest movements via social media (The Appeal) NYPD Social Media Monitoring Policy Allows For Use Of Aliases, Has Exceptions For Terrorist Activity (Tech Dirt) Stop and Frisk Online: Theorizing Everyday Racism in Digital Policing in the Use of Social Media for Identification of Criminal Conduct and Associations (Social Media + Society, Volume 3) The Strange Aftermath of the Largest Gang Bust in New York History (Vice) Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media (Oklahoma Law Review, Volume 71) The Wildly Unregulated Practice of Undercover Cops Friending People on Facebook (The Root) To Stem Juvenile Robberies, Police Trail Youths Before the Crime (The New York Times) Undercover cops break Facebook rules to track protesters, ensnare criminals (NBC News)

Criminal Group Database, aka the "Gang Database"

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
Gang databases contain information about individuals who police regard as confirmed or suspected gang members. The criteria for inclusion in the database are not always known, but can include poorly-defined activities such as associations with suspected gang members, various styles of dress, numerous clothing colors, and certain tattoos. In some instances, activity far removed from gang connections, such as drawing a high school mascot[21] or simply frequenting an area where gangs are known to assemble[22] has landed individuals in a gang database.	Gang databases raise the following concerns: **Racial Bias.** The vague and broad criteria for inclusion, open the door to racial bias. NYPD officials have acknowledged that as many as 95 percent of the people in its gang database are Black or Latinx.[23] **Impact on immigration status.** A gang affiliation can have negative consequences for an individual's interactions with federal immigration authorities. Immigration and Customs Enforcement (ICE) agents have been known to target individuals that have been identified as gang members in police databases.[24] The extent of information sharing between the NYPD and ICE is not properly understood. **False Positives.** Gang databases are notoriously inaccurate and over-inclusive. Individuals generally do not know if they are in the database, and there is not always a mechanism for challenging their inclusion.	There is no public NYPD policy. The information we know about the NYPD's use of the gang database comes from NYPD's testimony during city council proceedings. According to the NYPD, there are two ways individuals get added to the Gang Database: (1) Self-admission of "gang membership" to a member of the NYPD[25], being identified as a gang member by two "independent and reliable sources," or "social media posts admitting to membership in a gang." It is unclear whether NYPD requires a clear declaration of membership, or if vague associations perceived by investigating officers will do. (2) If any two of the following circumstances are true: (a) Frequent presence at a known gang location (this criteria may capture huge numbers of people who have no association besides residing in an area with active gang members); (b) Possession of "gang-related documents" (without more information, it is difficult to determine what kinds of "documents" are being referred to and whether there may be innocuous reasons to possess them); (c) Association with known gang members (it is possible to have friends and family who are gang members without joining it); (d) Social media posts with known gang members while possessing known gang paraphernalia, such as beads, flags, and bandanas (there are many reasons to pose with known gang members for social media, including for safety or familial ties); (e) Scars and tattoos associated with a particular gang; or (f) Frequently wearing colors and frequent use of hand signs that are associated with a particular gang. As of June 2018, the NYPD's gang database contained around 17,600 individuals, down from a high of 34,000.[26]	Groups Demand to See Criteria for NYPD Gang Database (Courthouse News Service) NYPD Gang Database Can Turn Unsuspecting New Yorkers into instant Felons (The Intercept) NYPD honcho insists gang database saves lives, but a teary City Council member said it can have devastating consequences (NY Daily News) How Gang Victims Are Labelled as Gang Suspects (The New Yorker) The Database (BRIC TV, Vimeo video) The fight against the NYPD gang database (The Policing and Social Justice Project, Youtube video) When a Facebook Like Lands You in Jail (Brennan Center) Spotlight: The Dangers of Gang Databases and Gang Policing (The Appeal)

Predictive Policing

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
There are two types of predictive policing programs: place-based and person-based. Place-based predictive policing uses algorithms to analyze data sets in order to try to predict where certain crimes are likely to occur. These estimates are used to inform where police officers are deployed. Person-based predictive policing analyzes data sets in order to generate a list of individuals an algorithm believes are likely to commit a crime.	Predictive policing raises the following concerns: **Racial Bias.** Predictive policing tools incorporate historical policing data to generate predictions. This makes it likely that these systems will recreate biased policing practices that have resulted in the over-policing of communities of color or data that has been manipulated to reflect higher or lower incidences of crimes. For example, historical NYPD arrest data may be tainted by its unconstitutional stop-and-frisk program or by data manipulation tactics such as falsifying arrest records to meet arrest quotas. **Privacy.** Predictive policing tools undermine constitutional requirements that police should target individuals based on individualized suspicion, not statistical probability.	There is no public NYPD policy, but the department has stated that its Public Security Privacy Guidelines for the Domain Awareness System govern predictive policing. These guidelines do not refer to predictive policing systems, and they describe the Domain Awareness System as a system to "monitor public areas and public activities," which does not describe predictive policing. The NYPD uses its own proprietary system that tries to locate hotspots for a particular crime based on an unknown number and type of data inputs.[27] Much of what we know about the NYPD's system comes from the Brennan Center's three-year legal fight with the NYPD over our public records request for documents about the development and use of the system. We do not have a complete picture of the system's inputs and outputs, but the NYPD says that its system "was not designed to store, maintain, or archive output predictions."[28] The failure to archive predictions frustrates the ability to study or audit the system for bias and related concerns. NYPD correspondence with potential vendors suggests an openness to using data inputs that could function as racial proxies, though it's not known if these inputs are incorporated into the NYPD's system. These include demographic data, school enrollment, educational attainment, income levels, journey to work, poverty levels, median income, and population under age 18.[29]	NYPD Predictive Policing Documents (Brennan Center) Predictive Policing Goes to Court (Brennan Center) 'Red Flags' as New Documents Point to Blind Spots of NYPD 'Predictive Policing' (The Daily Beast) Court: Public Deserves to Know How NYPD Uses Predictive Policing Software (Brennan Center) Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice (New York University Law Review Online) The New York City Police Department's Domain Awareness System (NYPD academic article)

Cell Site Simulators, aka "Stingrays"

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
Cell site simulators, also known as Stingrays or IMSI catchers, are devices that trick phones within a certain radius into connecting to the device rather than a cell tower, thus revealing their location to the operator of the device. Police departments use cell-site simulators to pinpoint the location of phones of targeted suspects. Cell-site simulators can also log IMSI numbers (unique identifying numbers) of all mobile devices within a given area. Additionally, while there is no evidence NYPD has used this functionality, some cell-site simulators can intercept communications that a phone is sending or receiving, and they can even change the content of those communications.[30]	Cell site simulators raise the following concerns: **Privacy.** Cell-site simulators can locate and track individuals as they move throughout public and private spaces, including when they are within a location that would require a warrant to enter. They are also indiscriminate, tricking every phone within their radius into providing identifying information. In a dense city like New York, this means numerous bystander devices will be picked up along with the targeted device. **Free Speech.** Without appropriate safeguards, cell-site simulators can be used to identify the individuals who attend protests or particular houses of worship.	There is no public NYPD policy. In 2017, a Brooklyn judge held that police use of Stingrays requires a warrant supported by probable cause.[31] Prior to this ruling, NYPD stated that its practice was to obtain a pen-register order — an order issued by a judge — so long as police can show reasonable suspicion.[32] Between 2008 and 2015, NYPD used Stingrays in over 1,000 investigations.[33] There is no publicly available information on whether the police purged extraneous data.	Cellphones, Law Enforcement, and the Right to Privacy (Brennan Center) Brooklyn Court: NYPD's Use of Cell-Phone Trackers Unconstitutional (Brennan Center) Did the Police Spy on Black Lives Matter Protesters? The Answer May Soon Come Out (The New York Times) New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says (The New York Times)

Automated License Plate Readers

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
Automated license plate readers (ALPRs) are devices that are attached to police cars or fixed on poles to capture the license plates of all cars passing by. License plate reads are also frequently run against a "hot list" of, for instance, stolen cars or AMBER Alerts. In addition to license plates, ALPRs can capture photographs of cars, along with photos of the driver and passengers. This information is uploaded to a database where it can be analyzed to study movements, associations, and relationships to crimes.	ALPRs raise the following concerns: **False Positives.** Information from ALPRs can be incorrect and lead to unnecessary and potentially dangerous police encounters. **Privacy.** ALPR data can provide a detailed account of an individual's movements. It can be used to target people who visit sensitive places, such as immigration clinics, protests, or houses of worship. **Impact on Immigration Status.** Police agencies can choose to share their ALPR information with federal immigration authorities. According to a public records request, ICE has received ALPR data from 80 different police departments, including Fairfield, CT; San Diego, CA; Orange County, Texas; and Athens-Clarke County, GA; among others.[34] It is not known whether the NYPD shares ALPR data with ICE, but the Public Security Privacy Guidelines permit the sharing of ALPR information with government entities.	Public Security Privacy Guidelines (2009). License Plate Reader Devices Operations Order (2013). The NYPD operates nearly 500 license plate readers as part of its Domain Awareness System,[35] and as of 2013, the department had a database of 16 million license plate reads.[36] The NYPD has used license plate readers to collect information about the cars parked in mosque parking lots.[37] Through its contract with the vendor Vigilant Solutions, the NYPD now has access to a database that contains over 2.2 billion license plate reads.[38] Vigilant Solutions has a national database of license plates, a national network of private ALPRs, and analytical tools that allow police to "stake out" areas, predict where certain individuals may be, and track individuals outside of New York City.[39] We do not currently know if NYPD shares the data it gets from its own ALPRs with other clients of Vigilant Solutions as well as other law enforcement or federal immigration agencies, as some cities do.	Documents Reveal ICE Using Driver Location Data From Local Police for Deportations (ACLU) Documents Uncover NYPD's Vast License Plate Reader Database (ACLU) Thousands of ICE employees can access license plate reader data, emails show (The Verge) License plate reader error leads to traffic stop at gunpoint, court case (Ars Technica) Data Driven: Explore How Cops Are Collecting and Sharing Our Travel Patterns Using Automated License Plate Readers (Electronic Frontier Foundation) Privacy advocate held at gunpoint after license plate reader database mistake, lawsuit alleges (The Verge)

Domain Awareness System

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
The Domain Awareness System (DAS) is a network of cameras, software, sensors, databases, devices, and related infrastructure that provides information and analytics to police officers for the purposes of “public safety” and to “detect, deter, and prevent potential terrorirst activities.”	DAS raises the following concerns: **Privacy.** DAS creates a system of persistence surveillance that covers vast swaths of New York City, which can be used to monitor the movements of New Yorkers as they move throughout the city. **False Positives.** False matches from various components, such as automatic license plate readers, can place innocent people at risk of dangerous police encounters.[40] **Data May be Shared.** The extent to which information obtained from the DAS is shared with federal agencies, such as immigration authorities, remains unknown.	The system’s Public Security Privacy Guidelines (2009) specify that the purpose of the DAS is to detect and prevent terrorist attacks, but the NYPD may use these technologies for ordinary police investigations, including the detection of loiterers.[41] The guidelines fail to cover technologies, such as video analytics, that have been incorporated since they were issued. The NYPD’s DAS collects and analyzes data from a variety of sources in lower and midtown Manhattan, including approximately: 9,000 CCTV cameras, some owned by the NYPD and some owned by private entities that share their feeds with police.[42] ▪ 500 license plate readers,[43] plus information obtained from contractor Vigilant Solutions.[44] ▪ Radiation and chemical sensors.[45] ▪ NYPD databases, including arrest records, criminal records, etc..[46] ▪ ShotSpotter coverage (see below for additional information).[47] ▪ 911 calls.[48]	How New York City is watching you (City & State New York) NYPD Domain Awareness System (DAS) (The Institute for Operations Research and the Management Sciences) The New York City Police Department’s Domain Awareness System (NYPD article, INFORMS Journal on Applied Analytics, Volume 47)

Drones

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
Drones are remotely operated aircraft — ranging in size — that can be equipped with various cameras, sensors, and other devices. For example, they can deploy cameras capable of facial recognition, and can also contain GPS trackers and Stingray devices.	Drones raise the following concerns: **Privacy.** Without proper oversight, drones can engage in forms of surveillance that can redefine reasonable expectations of privacy. Drones can also be used to collect information about bystanders who are not connected to a law enforcement investigation. These risks are largely invisible, as drones can be difficult for ordinary persons to detect or protect against depending on their size or altitude. **Free Speech.** Without proper oversight, drones can be deployed to surveill individuals in ways that chill free expression.	Patrol Guide: Use of Unmanned Aircraft System (2018). The NYPD’s policy specifies that it will not equip drones with facial recognition, but it contains a large carve-out for situations where there is a “public safety concern.”[49] It is unclear if there are any restrictions on running historical drone footage through a separate facial recognition system. The policy also specifies that drone footage will only be retained for 30 days, but it contains a carve-out that allows this period to be extended for various types of legal investigations.[50] According to the NYPD, the department deploys drones for uses such as crowd control, hostage situations, and reaching remote areas. The NYPD says drones will not be used for routine police patrols, to enforce traffic laws, or for “unlawful surveillance,[51] but the NYPD has deployed drones to monitor protesters at least once during the 2019 NYC Pride March.[52]	New York’s New Eyes in the Sky (Slate) New York Police Say They Will Deploy 14 Drones (The New York Times) Eyes In The Sky: The Public Has Privacy Concerns About Drones (Forbes) New NYPD Drone Policy Represents A Serious Threat to Privacy (New York Civil Liberties Union)

X-ray Vans

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
These vans use "Z backscatter" x-rays that bounce off objects, allowing the police to see into vehicles and behind walls as the van drives by.	X-ray vans raise the following concerns: **Privacy.** X-ray vans raise privacy and constitutional concerns, as they potentially allow police to examine intimate details of human bodies, private vehicles, and even inside homes. **Health.** X-ray vans raise health concerns as they may expose individuals to doses of ionizing radiation.	There is no public NYPD policy. The ways in which the NYPD uses x-ray vans and for which types of investigations remain largely unknown.[53]	Split Decision on NYPD's X-ray Vans (ProPublica) NYPD has super-secret X-ray vans (New York Post) Public Sees Through NYPD X-Ray Vans (Policing Project at NYU School of Law) The NYPD Is Using Mobile X-Ray Vans to Spy on Unknown Targets (The Atlantic)

Gunshot Detection System (ShotSpotter)

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
The privately developed ShotSpotter system uses sensors to pick up sounds that appear to be gunshots. Audio snippets are automatically sent to vendor employees who attempt to verify whether the sound represents a shooting. The vendor employee then transmits information about the potential shooting to police department clients.	Gunshot detection systems raise the following concerns: **False Positives.** This system can make mistakes and confuse ordinary background noise as gunshots. **Privacy.** Recordings of ambient noise can be misued to target voice surveillance by recording audio from selected ShotSpotter devices.	There is no standalone NYPD policy, but it may be subject to the DAS's Public Security Privacy Guidelines, since gunshot detection systems are incorporated into the NYPD's Domain Awareness System. The NYPD's ShotSpotter system uses sensors that triangulate the location of sounds that may be gunshots. If a ShotSpotter employee believes a shooting occurred, the system then sends data, including audio of the incident, to the Domain Awareness System.[54] Cameras within 500 feet are programmed to capture footage before and after the suspected gunshot.[55] Investigators at the NYPD Domain Awareness System then transmit relevant data to field officers.[56]	Here's How the NYPD's Expanding ShotSpotter System Works (DNAinfo) Privacy Audit & Assessment of ShotSpotter, Inc.'s Gunshot Detection Technology (Policing Project at NYU School of Law) The NYPD's newest technology may be recording conversations (Business Insider)

DNA Database aka the Local DNA Index System

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
DNA databases contain genetic information about individuals, which can be analyzed against a suspect's DNA for a potential match. According to media reports, the NYPD's DNA database contains as many as 82,473 genetic profiles, including samples obtained from children.[57]	DNA databases raise the following concerns: **Privacy.** Biometric samples for DNA databases can be collected without appropriate standards that respect individual privacy. Individuals are not always given a full and accurate representation of how their genetic profile will be used, and there are often no protocols for deletion. In addition, voluntary samples can be collected from children that are incapable of giving informed consent. Finally, the secret collection of "abandoned" genetic samples means that many individuals have no notice that their genetic information was collected and added to a city database. **Racial Bias.** Communities of color are likely overrepresented in DNA databases resulting from overpolicing of specific communities.	Detective Guide (2013) contains redacted instructions for collecting "abandoned" DNA samples in both "controlled" and "uncontrolled" environments. Chief of Detectives Memo #17 (2010). The memo contains instructions for how to collect "abandoned" DNA samples from objects such as water bottles, bubble gum, and apples for submission to Office of the Chief Medical Examiner (OCME) for examination. Many individuals in DNA databases have never been accused or convicted of any crime, and there are limited avenues for impacted indivudials to request deletion. There are three methods for the NYPD to obtain biometric samples for DNA analysis: ■ **Voluntary sample.** Officers can ask individuals to provide a biometric sample for DNA analysis, but they are not necessarily required to disclose that it may be used for an unlimited number of investigations and that the sample will be retained indefinitely. They are also not required to tell individuals that they are allowed to refeuse consent. At times, police collect biometric samples from children without a lawyer, parent, or guardian present. One New York State court ruled that the NYPD violated a minor's Fourth Amendment rights against unreasonable search and seizure when they collected a genetic sample for DNA analysis where they received a written consent from the minor without the presence of his parent, guardian, or attorney.[58] ■ **Secret collection of "abandoned" samples.** NYPD officers will obtain "abandoned" genetic samples from discarded objects, such as water bottles, chewing gum, and apples. For example, police officers bring suspects into interrogation rooms, wait for the suspect to take a drink or smoke a cigarette, and collect the sample once a suspect throws the object away.[59] ■ **Court-ordered collection.** A court will order a suspect to provide a sample for DNA profiling where the prosecution can establish: "(1) probable cause to believe the suspect has committed the crime. (2) a 'clear indication' that relevant material evidence will be found, and (3) the method used to secure it is safe and reliable."[60]	N.Y.P.D. Detectives Gave a Boy, 12, a Soda. He Landed in a DNA Database (The New York Times) NYPD detectives demanded DNA swabs from hundreds of black and Latino men while hunting killer of Howard Beach jogger (NY Daily News) How Juveniles Get Caught Up In The NYPD's Vast DNA Dragnet (Gothamist) Legal Aid Society is Working to Protect New Yorkers From 'Genetic Stop and Frisk' (NowThis News) Push to solve gun cases fuels rapid growth of New York's DNA database (NY Daily News) New York Examines Over 800 Rape Cases for Possible Mishandling of Evidence (The New York Times) Can DNA Evidence Be Too Convincing? An Acquitted Man Thinks So (The New York Times) In New York City, Gun Cases Fuel Growing, Unregulated DNA Database (The Trace) City's DNA database swells as cops log New Yorkers' genetic material (Queens Daily Eagle) OCME Laboratory Protocols (NYC Office of Chief Medical Examiner)

Body Cameras

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
Body cameras are used to record an officer's interactions with the public and store the video for future review or use in criminal or civil proceedings. While body cameras have been promoted as a tool for police accountability, they have largely functioned as evidence-gathering devices.	Body cameras raise the following concerns: **Effectiveness.** As part of the settlement related to the NYPD's unconstitutional stop-and-frisk program, a federal judge ordered the NYPD to develop a mechanism for officers to electronically record certain police encounters.[61] However, the cameras remain under the control of police, who can decide when to activate them. Even when the cameras are rolling, police officers can add audio commentary that skews public perception of an incident (e.g. yelling "stop resisting" to a cooperating person). **Privacy.** Absent safeguards, body cameras can function as mobile surveillance devices, recording information about people and places that officers encounter while on patrol, regardless of their relationship to a suspected crime. Future iterations of body cameras may be equipped with facial recognition technology,[62] raising additional concerns about privacy, effectiveness, and racial bias.	Body Camera Patrol Guide (2018). All uniformed patrol officers in New York City are equipped with body-worn cameras.[63] In New York City, members of the public can request video under the Freedom of Information Act, but when it relates to evidence in a criminal case the video is turned over to the prosecutor's office. If a camera records an officer-involved shooting or other high-profile incident, NYPD works with "relevant authorities" to determine if video can be made public.[64]	Body cameras can't solve all our problems (USA Today) A Big Test of Police Body Cameras Defies Expectations (The New York Times) Body-Worn Cameras: What you need to know (NYPD) The benefits of police body cams are a myth (TechCrunch) Police Body Worn Cameras: A Policy Scorecard (The Leadership Conference & Upturn) NYPD Completes Rollout of Body-Worn Cameras to All Officers on Patrol (NYPD) The Hidden Bias of Cameras (Slate)

SkyWatch & TerraHawk Surveillance Towers

How It Works	Impact	NYPD Policy & Scope of Use	Further Reading
Surveillance towers allow officers to monitor areas from several stories above street level as well as record movements within a targeted area. Each SkyWatch tower contains flood lights, a command desk, devices to detect vehicle speeds, tinted windows, digital video recorders, and customized surveillance cameras.[65] The standard equipment placed on TerraHawk towers is unknown, but their patented technology contemplates the use of surveillance cameras along with infrared detectors, motion detectors, and a thermal imaging device.[66]	Surveillance towers raise the following concerns: **Privacy.** Surveillance towers impose a feeling of persistent monitoring, challenging reasonable expectations of privacy. Surveillance towers can also be used to collect information about bystanders who are not connected to a law enforcement investigation. **Free Speech.** Persistent monitoring from surveillance towers can chill associations among individuals.	SkyWatch Detective Guide (2013), redacted. TerraHawk Detective Guide (2013), redacted. NYPD may deploy surveillance towers in response to a rise in crime within a particular area,[67] but they have also been used to monitor protests, such as Occupy Wall Street.[68] The current number of towers deployed by NYPD is unknown. Surveillance towers are also used to collect "probative" and "potentially probative" images, according to patrol guides, but the meaning of these terms is unclear. According to media reports, TerraHawk Towers have been deployed in Staten Island, Far Rockaway, Coney Island, and Howard Beach. [69] SkyWatch have also been deployed in Harlem[70], Crown Heights[71], downtown Manhattan (Zuccotti Park)[72], Bedford-Stuyvesant Brooklyn[73], and the Lower East Side of Manhattan (Tompkins Square Park)[74].	Brooklyn Bureau: NYPD Towers May Defuse Cop, Community Friction (City Limits) NYPD Removes Controversial Surveillance Tower From Tompkins Square Park (Observer)

Endnotes

[1] *See*, e.g., Joy Buolamwini and Tim Gerbu, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,” available at: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; *See also* Abdurrahim, S.H., Samad, S.A. & Huddin, A.B. Vis Comput (2018) 34: 1617, available at: https://doi.org/10.1007/s00371-017-1428-z; *See also* Jacob Snow, “Amazon’s Face Recognition False Matched 28 Members of Congress with Mugshots,” available at: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

[2] *See* Coalition letter urging federal moratorium on face recognition for law enforcement and immigration enforcement purposes, available at: https://www.aclu.org/sites/default/files/field_document/2019-06-03_coalition_letter_calling_for_federal_moratorium_on_face_recognition.pdf.

[3] San Francisco “Stop Secret Surveillance” ordinance, File No. 190110, available at: https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A.

[4] The final revisions to Oakland’s Surveillance and Community Safety Ordinance are pending, but *see* Charlie Osborne, “Oakland follows San Francisco’s lead in banning facial recognition tech,” ZDNet, July 19, 2019, available at: https://www.zdnet.com/article/oakland-city-follows-san-franciscos-lead-in-banning-facial-recognition-tech/.

[5] *See* City of Somerville Massachussetts Agenda Item 207566, available at: http://somervillecityma.iqm2.com/Citizens/Detail_LegiFile.aspx?Frame=&MeetingID=2941&MediaPosition=&ID=20375&CssClass=.

[6] *See* NYPD correspondence with DataWorks Plus, Document 020238-020312 at page 74-75 available at: https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22.

[7] NYPD, *Real Time Crime Center FIS Presentation*, available at: https://drive.google.com/open?id=18yVMSMAblqcE_nAIGf9XRIUnik8xWOh_.

[8] *See id*.

[9] *See id*.

[10] NYPD, Real Time Crime Center Facial Identification Section (FIS), presentation by Detective Markiewicz (Sept. 17, 2018) (notes on file with Clare Garvie at Georgetown Law Center on Privacy & Technology).

[11] *See* George Joseph and Kenneth Lipp, “IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search By Skin Color,” *The Intercept*, September 6, 2018, available at: https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/; *see also* IBM Presentation to NYPD “IBM SVS 4.0 Research and Development Status Update 6 for NYPD,” (hereinafter “IBM Presentation”) October 16, 2012, available at: https://www.documentcloud.org/documents/4452844-IBM-SVS-Analytics-4-0-Plan-Update-for-NYPD-6.html.

[12] *See* Vexcel Presentation “Vexcel – NYPD: Domain Awareness System; IBM Delivery Transition Review,” at slide 3, available at: https://www.documentcloud.org/documents/4452846-Vexcel-NYPD-DTR-02-04-10.html.

[13] IBM, Software withdrawal: IBM Intelligent Video Analytics, April 23, 2019, available at: https://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/2/897/ENUS919-092/index.html&request_locale=en.

[14] *See* Statements of NYPD Inspector Salvatore DiPace, “New York City’s Hidden Surveillance Network Part 2 – by Scientific American,” September 16, 2011, available at: https://www.youtube.com/watch?v=LSf4YCB3Hi0I; *see also* IBM Presentation at slide 22-50.

[15] George Joseph and Kenneth Lipp, “IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search By Skin Color,” *The Intercept*, September 6, 2018, available at: https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/.

[16] 2017 Handschu Guidelines at Section IX(B)(1), available at: https://www.aclu.org/sites/all/libraries/pdf.js/web/viewer.html?file=https%3A%2F%2Fwww.aclu.org%2Fsites%2Fdefault%2Ffiles%2Ffield_document%2Fraza_exhibit_a_to_order_approving_stipulation_of_settlement_revised_handschu_guidelines.pdf#page=1&zoom=auto,-14,800

[17] *See id*. at Section IX(B)(2).

[18] *See* Office of Community Oriented Policing Services, U.S. Department of Justice and Police Executive Research Forum, “Social Media and Tactical Considerations” at 13 (2013) (identifying NYPD units that engage in social media monitoring, and exploring use by Intelligence and Juvenile Justice as case studies), available at: https://www.policeforum.org/assets/docs/Free_Online_Documents/Technology/social%20media%20and%20tactical%20considerations%20for%20law%20enforcement%202013.pdf.

[19] *See* David Uberti, “How Social-Media Surveillance of Teenagers Led to a New King of Policing,” *The Nation*, April 19, 2019, available at: https://www.thenation.com/article/jeffery-lane-digital-street-book-review/.

[20] *See id*. at 13-16; *see also* George Joseph, “Years After Protests, NYPD Retains Photos of Black Lives Matter Activists,” The Appeal, January 17, 2019, available at: https://theappeal.org/years-after-protests-nypd-retains-photos-of-black-lives-matter-activists/.

[21] *See* Hannah Dreier, “He Drew His School Mascot – and ICE Labeled Him a Gang Member,” *ProPublica*, December 27, 2018, available at: https://features.propublica.org/ms-13-immigrant-students/huntington-school-deportations-ice-honduras/.

[22] *See* Ali Winston “Vague Rules Let Ice Depoart Undocumented Immigrants as Gang Members” *The Intercept*, February 17, 2017, available at: https://theintercept.com/2017/02/17/loose-classification-rules-give-ice-broad-authority-to-classify-immigrants-as-gang-members/.

[23] *See* Jeff Coltin, “Why everyone is suddenly talking about the NYPD gang database,” City & State New York, June 13, 2018, available at: https://www.cityandstateny.com/articles/policy/criminal-justice/why-everyone-suddenly-talking-about-nypd-gang-database.html.

[24] Emmanuel Felton, “Gang Databases Are a Life Sentence for Black and Latino Communities,” *Pacific Standard*, March 15, 2018, available at: https://psmag.com/social-justice/gang-databases-life-sentence-for-black-and-latino-communities.

[25] *See* Statement of Chief Dermot Shea, Chief of Detectives, New York City Police Department, Before the New York City Council Committee on Public Safety, Committee Room, City Hall, June 13, 2018, at 4.

[26] *See id*.

[27] *See* E.S. Levine, Jessica Tisch, Anthony Tasso, and Michael Joy, “The New York City Police Department’s Domain Awareness System,” Informs Journal on Applied Analytics, January 18, 2017, available at: https://pubsonline.informs.org/doi/10.1287/inte.2016.0860 (subscription required).

[28] *See* Affidavit of Lesa Moore, Supreme Court of the State of New York, County of New York, Index No. 160541/2016 at Page 2, available at: https://www.brennancenter.org/sites/default/files/Lesa%20Moore%20Affidavit%20in%20Compliance%20-FINAL%20-%20%28%23%20Legal%209761080%29%20%281%29.pdf.

[29] *See* Predictive Forecasting of Crime, a KEYSTATS presidenation

for the New York City Police Department, at 2-7, available at http://www.brennancenter.org/sites/default/files/Keystats%20Desired%20Data%20Elements.pdf.

[30] *See* Promotional Material from GammaGroup, "3G-GSM Tactical Interception & Target Location," available at: https://info.publicintelligence.net/Gamma-GSM.pdf.

[31] *See New York v. Gordon*, 58 Misc.3d 544, 550-51 (2017), available at http://www.nycourts.gov/reporter/3dseries/2017/2017_27364.htm.

[32] *See id*, *see also* NYPD FOIL Response to Request #15-PL-3861 at 4, available at: https://www.nyclu.org/sites/default/files/releases/NYPD%20FOIL%20Appeal%20Response%20Stingrays.pdf.

[33] *See* NYPD response to NYCLU FOIL Request, available at: https://www.nyclu.org/sites/default/files/releases/NYPD%20Stingray%20use.pdf.

[34] *See* Vasudha Talla, "Documents Reveal ICE Using Driver Location Data From Local Police for Deportations", March 13, 2019, available at: https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data.

[35] *See* Testimony of Deputy Commissioner of Intelligence and Counterterrorism John J. Miller, New York City Policy Department, Before the New York City Council Committees on Public Safety and Fire and Criminal Justice Services, November 12, 2014, at 4.

[36] *See* Joseph Goldstein, "Weekly Police Briefing Offers Snapshot of Department and Its Leader," *The New York Times*, February 10, 2013, available at: https://www.nytimes.com/2013/02/11/nyregion/weekly-briefing-provides-lengthy-snapshot-of-kelly-and-nypd.html?_r=0.

[37] *See* Adam Goldman and Matt Apuzzo, "With cameras, informants, NYPD eyed mosques," *Associated Press*, February 23, 2012, available at: https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques.

[38] *See* Mariko Hirose, "Documents Uncover NYPD's Vast License Plate Reader Database," ACLU, January 25, 2016, available at: https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-reader-database.

[39] *See* Agreement Between New York City Police Department and Vigilant Solutions for License Plate Recognition Data & Law Enforcement Archival & Reporting Network, dated as of April 9, 2015 at Exhibit 1 (Contractor Scope of Work), available at: https://www.nyclu.org/sites/default/files/20150409_NYCC_ALPR_foil.pdf

[40] *See* Colin Lecher, "Privacy advocate held at gunpoint after license plate reader database mistake, lawsuit alleges," *The Verge*, February 21, 2019, available at: https://www.theverge.com/2019/2/21/18234785/privacy-advocate-lawsuit-california-license-plate-reader.

[41] *See* NYPD Public Security Privacy Guidelines, April 2, 2009 at Pages 2-3, available at: https://www1.nyc.gov/assets/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf

[42] *See* Testimony of Deputy Commissioner of Intelligence and Counterterrorism John J. Miller, New York City Policy Department, Before the New York City Council Committees on Public Safety and Fire and Criminal Justice Services, November 12, 2014, at 4.

[43] *Id.*

[44] *See* Agreement Between New York City Police Department and Vigilant Solutions for License Plate Recognition Data & Law Enforcement Archival & Reporting Network, dated as of April 9, 2015 at Exhibit 1 (Contractor Scope of Work), available at: https://www.nyclu.org/sites/default/files/20150409_NYCC_ALPR_foil.pdf

[45] *Id.*

[46] *See* Thomas H. Davenport, "How Big Data is Helping the NYPD Solve Crimes Faster," Fortune, July 17 2016, available at: http://fortune.com/2016/07/17/big-data-nypd-situational-awareness/.

[47] *See id*.

[48] *See id*.

[49] *See* William Alden, "There's a Fight Brewing Between the NYPD and Silicon Valley's Palantir," BuzzFeed News, June 28, 2017, available at: https://www.buzzfeednews.com/article/williamalden/theres-a-fight-brewing-between-the-nypd-and-silicon-valley; *see also* NYPD Patrol Guide: Use of Department Unmanned Aircraft System (UAS), available at: https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/public-pguide2.pdf#page=687.

[50] *See id*.

[51] *See* Ashley Southall and Ali Winston, "New York Police Say They Will Deploy 14 Drones," *The New York Times*, December 4, 2018, available at: https://www.nytimes.com/2018/12/04/nyregion/nypd-drones.html.

[52] Noah Manskar, "NYC Pride March Will Be Especially Huge for Stonewall Anniversary," *Patch*, June 25, 2019, available at: https://patch.com/new-york/new-york-city/nyc-pride-march-will-be-especially-huge-stonewall-anniversary.

[53] *See In the Matter of Grabell v. New York City Police Department*, 139 A.D.3d 477, 479 (2016).

[54] *See* NYPD Technology: Helping the Finest Keep NYC Safe," February 17, 2017, available at: http://nypdnews.com/2017/02/nypd-technology-helping-the-finest-keep-nyc-safe/.

[55] *See* Rocco Parascandola and Oren Yaniv, "De Blasio, NYPD Unveil $1.5M ShotSpotter system, detects gunshots via sensors around city and alerts police automatically," *New York Daily News*, March 16, 2015, available at: https://www.nydailynews.com/new-york/nypd-unveils-1-5m-shotspotter-system-bronx-article-1.2151679.

[56] *See* NYPD Technology: Helping the Finest Keep NYC Safe," February 17, 2017, available at: http://nypdnews.com/2017/02/nypd-technology-helping-the-finest-keep-nyc-safe/.

[57] *See* Jan Ransom and Ashley Southall, "N.Y.P.D. Detectives Gave a Boy, 12, a Soda. He Landed in a DNA Database," *The New York Times*, August 15, 2019, available at: https://www.nytimes.com/2019/08/15/nyregion/nypd-dna-database.html.

[58] *See People v. K.M.,* 2018 N.Y. Slip Op. 28363 at *6.

[59] *See, e.g. People v. Blank,* 2018 N.Y. Slip Opp 28274.

[60] *See Matter of Abe A.*, 56 N.Y.2d 288, 291 (1982).

[61] *See Floyd. v. City of New York,* Case 1:08-cv-01034-AT, Document 619 "Order Regarding Documenting Police-Citizen Encounters," July 19, 2018, available at: https://www.naacpldf.org/wp-content/uploads/Order-re-lower-level-doc-pilot_0.pdf.

[62] Axon, a leading manufacturer of body cameras, has said it will ban the use of facial recognition in its products because the "technology is not yet reliable enough." *See* First Report of the Axon AI & Policing Technology Ethics Board, available at: https://www.policingproject.org/axon.

[63] New York City Police Department Newsroom, "NYPD Completes Rollout of Body-Worn Cameras to All Officers on Patrol," March 6, 2019, available at: https://www1.nyc.gov/site/nypd/news/pr0306/nypd-completes-rollout-body-worn-cameras-all-officers-patrol#/0.

[64] *See* Body-Worn Cameras, What you need to know, available at: https://www1.nyc.gov/site/nypd/about/about-nypd/equipment-tech/body-worn-cameras.page.

[65] *See* FLIR SkyWatch Options, available at: https://www.flir.com/globalassets/imported-assets/document/skywatch-options.pdf.

[66] *See* TerraHawk, LLC patent for "Vehicle for deploying a mobile surveillance module," available at: https://patents.justia.com/patent/9669690.

[67] *See* e.g., Jen Chung, "After Bloody Weekend, NYPD Beefs Up Patrols, SkyWatch Towers," Gothamist, June 4, 2013, available at: https://gothamist.com/2013/06/04/after_bloody_weekend_nypd_beefs_up.php.

[68] *See* Tana Ganeva, "Is all that NYPD surveillance legal?" Salon, November 4, 2011, available at: https://www.salon.com/2011/11/04/is_all_that_nypd_surveillance_legal/.

69 *See* Andy Cush, "Here's the Newest Tool in the NYPD's Surveillance Arsenal," Animal New York, November 15, 2012, available at: http://animalnewyork.com/2012/heres-the-newest-tool-in-the-nyps-surveillance-arsenal/.

70 *See* "NYPD Installs 'Sky Watch' in Harlem Neighborhood," CrownHeights.info, November 23, 2006, available at: http://crownheights.info/crime/3780/nypd-installs-sky-watch-in-harlem-neighborhood/.

71 *See id*.

72 *See* Nick Turse, "What Happened When I Tried to Get Some Answers About the Creepy NYPD Watchtower Monitoring OWS," AlterNet, November 6, 2011, available at: https://www.alternet.org/2011/11/what_happened_when_i_tried_to_get_some_answers_about_the_creepy_nypd_watchtower_monitoring_ows/.

73 *See* Orsianmi Burton, "An encounter with "SkyWatch" on a block in Bedford-Stuyvesant, Brooklyn, Anthropoliteia, May 8, 2014, available at: https://anthropoliteia.net/2014/05/08/an-encounter-with-sky-watch-on-a-block-in-bedford-stuyvesant-brooklyn/.

74 *See* Catherine Rafter, "NYPD Removes Controversial Surveillance Tower from Tompkins Square Park, The Observer, July 28, 2015, available at: https://observer.com/2015/07/nypd-removes-controversial-surveillance-tower-from-tompkins-square-park/.