Forums on NYPD Use of Surveillance Technology

Hosted by
Eisenberg & Baum, LLP

EB

Wednesday, February 10th, at 6:00 PM
Wednesday, February 17th, at 6:00 PM

Cell-Site Simulators (aka “Stingrays”)

Disclosed Usage	Cell-site simulators are used to locate or identify mobile devices. The technology supports locating missing persons, victims of abductions, and criminal suspects. Cell-site simulators can collect and share cellular device location data with NYPD investigators.
Concerns	Cell-site simulators can locate and track individuals as they move throughout public and private spaces. The usage of cell-site simulators are discretionary decisions. When police make decisions about how and where to apply the tool, it might be affected by their experience with past criminal patterns. Such information in turn might lead to further discriminatory use of the tool. Cell-site simulators indiscriminately trick every phone within their radius into providing identifying information. This is particularly problematic in a dense city like New York, where numerous bystander devices will be tracked. The technology can be used to identify individuals who attend protests.
Further Reading	1. How Cops Can Secretly Track Your Phone (The Intercept) 2. Brooklyn Court: NYPD’s Use of Cell-Phone Trackers Unconstitutional (Brennan Center for Justice)

Criminal Group Database

Disclosed Usage	It provides investigators with information about alleged gang members and additional intelligence relating to street gangs. It centralizes vital criminal group related intelligence that would otherwise be kept throughout different isolated data compartments within the NYPD. Entry into the Criminal Group Database is not proof of criminal behavior; it is only an investigative lead. Recommendations are reviewed by a supervisor in a Detective Bureau Gang Squad who will either approve or reject the recommendation or request additional analysis by the Department’s Gang Analysis Section.
Concerns	The Criminal Group Database disproportionately affects racial minority groups. NYPD officials have acknowledged that as many as 95 percent of the people in its criminal gang database are Black or Latinx. The information in the database reflects the past information about arrests and other experiences. The past arrests might show strong correlation with the allocation of police resources. For example, historical NYPD information about the gangs may be affected by over policing in some residential areas of racial minority groups. Moreover, law enforcement is not required to have a warrant or a probable cause to use the database. If such information is used to assist future decisions (e.g. whether to add a person to the database), it might lead to further discretionary arrest patterns against the same neighborhoods and groups of people. Criminal group databases are notoriously inaccurate and over-inclusive. Generally, individuals also do not know if they are in the database. The criteria to enter someone into a gang database are overly vague and broad. Young people who have not been arrested or accused of any criminal activity have been added to criminal group databases.

Further Reading	1. Groups Urge NYPD Inspector General to Audit the NYPD "Gang Database." (Human Rights Watch) 2. Police Surveillance Spurs Call for Youth Digital 'Bill of Rights' (The Crime Report) 3. Why everyone is suddenly talking about the NYPD gang database (City & State New York) 4. Damning Report On NYPD Gang Database Increases Calls To End 'A Tool of Mass Criminalization' (Gothamist)

Facial Recognition

Disclosed Usage	The facial recognition investigator will run a search using a facial recognition program for comparison of the probe image to images lawfully obtained by the NYPD. The program generates a pool of possible match candidates. The investigation does not solely depend on facial recognition.
Concerns	Representation of racial groups in the compared images affects the match rate of facial recognition. Police officers might collect images through body cameras about people who they encounter during daily tasks, such as street encounters and information-producing conversations. These collected images are not randomly distributed. Once being added into the database, it might appear as objective information even though they might come from over-policing or individual discretionary decisions. Facial recognition often misidentifies Black people and ethnic minorities, young people, and women at higher rates than white people, older people, and men, respectively. If systems that rely on criminal databases, like mugshot databases, will disproportionately target Black people, Latinos, and immigrants. Facial recognition systems with real-time surveillance capabilities can have a chilling effect on the freedom of speech and expression. Facial recognition systems employed by law enforcement generally does not require a warrant.
Further Reading	1. Garbage In, Garbage Out (Georgetown Law Center on Privacy & Technology) 2. The NYPD has a surveillance problem (City & State New York) 3. Face Off: Law Enforcement Use of Face Recognition Technology (Electronic Frontier Foundation)

ShotSpotter

Disclosed Usage	It can determine whether the sound was gunfire or a similar noise, like fireworks or a car backfiring. Once a gunfire is identified, it sends out notice to the police with location information. ShotSpotter has undergone a privacy audit at NYU Law.
Concerns	Free Speech and Association concerns: ShotSpotter has been used to detect fireworks, resulting in overpolicing non-violent crimes in areas that are dominantly communities of color. In the summer of 2020, fireworks were used by some BLM protesters in demonstrating solidarity, leading to concentrated policing toward protest groups.

	Disparate Impact concerns: The concentrated deployment of the tool in certain areas of the city can disproportionately impact racial minority groups and individuals of color. Higher numbers of ShotSpotters are installed in areas associated with gun violence in the past. The technology has shown more false positives and inaccuracies in these areas, where the majority of residents are individuals of color.
Further Reading	1. How police surveillance technologies act as tools of white supremacy (Phys.org) 2. Police Departments Are Using Gunshot-Tracking Technology To Pinpoint Fireworks (BuzzFeed News) 3. Gunshot detection technology raises concerns of bias and inaccuracy (Coda) 4. Privacy Audit & Assessment of ShotSpotter, Inc.'s Gunshot Detection Technology (Policing Project at NYU Law)

Social Network Analysis Tools

Disclosed Usage	Social network analysis tools automate the process of reviewing, retaining, and processing audio, video images, location, or similar information contained on Social Networking Platforms such as Twitter, Instagram, and Facebook. Enables the NYPD to retain information and alert investigators to new activity on queried social media accounts. The automated data retention allows NYPD to track information related to deleted and deactivated accounts, even when the social media user deletes certain information. The NYPD does not seek court authorization prior to using social network analysis tools. The data collected comprises publicly available information or information that is viewable as a result of user-selected privacy settings or practices.
Concerns	Police monitoring of social media may result in mass surveillance based on political, religious viewpoints. There is also a risk of a chilling effect on free speech and free association rights of individuals. Like other tools employed by law enforcement, social network analysis tools will disproportionately affect certain groups, particularly racial minority groups and activists. If social media data is being mined and analyzed, personal data privacy concerns arise as well, including the possibility that data may be shared with other governmental agencies.
Further Reading	1. How to reform police monitoring of social media (The Brookings Institution) 2. The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing (Harvard Law & Policy Review)

Data Analysis Tool

Disclosed Usage	Data Analysis Tools allow the NYPD to organize, process, and search within and across datasets from significant quantities of data generated by daily operations of the NYPD. Some data analysis tools utilize artificial intelligence and machine learning to identify connections between data points in isolated data compartments. Court authorization is not required for NYPD's use of data analysis tools, and may be used in any situation deemed appropriate by supervisory personnel. Data and information can be shared with other government agencies on a case by case basis. Access will not be given to other agencies for purposes of furthering immigration enforcement.
Concerns	Predictive policing uses algorithms that analyze high volumes of information to predict potential future crimes and allocate resources to prevent them. Data Analysis Tools, including predictive policing tools, may incorporate biases based on the data that is input. For example, if data and information collected are based on historic arrests and street encounters, it may disproportionately target communities and individuals of color and immigrants. The disproportionate results of the tools may lead to more concentrated data mining and allocation of police resources targeting communities and individuals of color, creating a pernicious feedback loop that reinforces bias. Data Analysis Tools also raise Fourth Amendment concerns. Police officers may rely upon a computer-hunch without an explanation, and the information is prone to confirmation bias and retroactive justifications that may supplant a proper probable cause determination.
Further Reading	1. Predictive Policing Explained (Brennan Center for Justice) 2. Summary of Agency Compliance Reporting (NYC Algorithms Management and Policy Officer) 3. A Bias-Free Predictive Policing Tool?: An Evaluation of the NYPD's Patternizr (Fordham Urban Law Journal)

Domain Awareness System

Disclosed Usage	DAS is one of the world's largest networks of cameras, license plate readers, and radiological censors, designed to detect and prevent terrorist acts, and used in criminal investigations. The network is a centralized repository of information from CCTV, License Plate Readers, ShotSpotter, and more. The Domain Awareness System (DAS) allows officers to access critical information relevant to ongoing security and public safety efforts, employing the resources of the private sector and other city agencies. DAS can share video images, location, and acoustic data with NYPD personnel who can access the data through their mobile device. The system provides officers with critical alerts on any issues or potential threats at queried locations.

Concerns	All of the concerns surrounding CCTV, ShotSpotter, and license plate readers, including false positives, over-policing, and racially discriminatory impact are similarly found in the use of DAS. Privacy Rights: DAS collects data of citizens from more than 20,000 CCTV cameras, police-worn body cameras, license plate readers, radiation scanners, drones, 911 calls, and unknown commercial and interagency intelligence databases, allowing for mass surveillance over the city. DAS has real-time tracking capabilities but can keep information indefinitely. Right to speech and association: During protests, images and data of protesters through were collected through surveillance technology dispersed in the city. Financial Burden: DAS was the largest NYPD spending, a total of $31.4 million, for Fiscal 2020. Vendor Integrity & Transparency: Microsoft and its partner Genetec have been criticized for surreptitiously selling its facial recognition and cloud services.
Further Reading	1. Microsoft needs to stop selling surveillance to the NYPD (Fast Company) 2. NYPD Black Lives Matter Surveillance (CNN) 3. Ditch DAS Letter (STOP.org and other Organizations)