Brooklyn Defenders

Brooklyn Defender Services
177 Livingston St, 7th Fl
Brooklyn, NY 11201

Tel (718) 254-0700
Fax (347) 457-5194
info@bds.org

TESTIMONY OF

Talia Kamran, Staff Attorney,

Seizure and Surveillance Defense Project

BROOKLYN DEFENDER SERVICES

Presented before

The New York City Council

Committees on Public Safety, Technology, and Oversight and Investigation

Oversight - Examining NYPD's Implementation of the POST Act

February 19, 2025

My name is Talia Kamran and I am a Staff Attorney and Equal Justice Works Fellow in the Seizure and Surveillance Defense Project at Brooklyn Defender Services. Brooklyn Defender Services (BDS) is a public defense office whose mission is to provide outstanding representation and advocacy free of cost to people facing loss of freedom, family separation and other serious legal harms by the government. We are grateful to the Committees on Public Safety, Technology, and Oversight and Investigation, and Chairs Salaam, Gutiérrez, and Brewer, for inviting us to testify today about the NYPD's compliance with the POST Act.

For nearly 30 years, BDS has worked, in and out of court, to protect and uphold the rights of individuals and to change laws and systems that perpetuate injustice and inequity. We represent approximately 23,000 people each year who are accused of a crime, facing loss of liberty, their home, their children, or deportation. Our staff consists of attorneys, social workers, investigators, paralegals and administrative staff who are experts in their individual fields. BDS also provides a wide range of additional services for our clients, including civil legal advocacy, assistance with educational needs of our clients or their children, housing and benefits advocacy, as well as immigration advice and representation.

Many of the people that we serve live in heavily policed and highly surveilled communities. These communities bear the brunt of the New York Police Department's (NYPD) privacy-destroying and abusive behavior, including through the wrongful seizure of their personal belongings, the unannounced addition of their deeply personal information (including DNA profiles, social networks, and every day habits) into unregulated law enforcement databases like

the gang database, and the unceasing subjection of "the privacies of life"[1] to police gaze through cameras, sensors, microphones, digital scraping tools, and their underlying, mass-aggregating databases like the Domain Awareness System (DAS).

The need for stringent oversight of the NYPD surveillance given this reality cannot be overstated. We are living in a city with Orwellian levels of surveillance. The NYPD has the capability—and actively uses it—to observe citizens constantly through an extensive network of CCTV cameras, as indicated in its DAS and CCTV Impact and Use Policies (IUPs). Now, with a vast array of drones equipped with audiovisual capabilities, this near-constant surveillance has become even more pervasive. This unchecked expansion of surveillance technology has serious implications for civil liberties and privacy rights, disproportionately affecting Black, brown, and low-income communities. In fact, similar practices have been found unconstitutional in other parts of the country, yet New York City continues to allow the NYPD to operate with little oversight.[2]

The Public Oversight of Surveillance Technology (POST) Act was enacted in 2020 in response to the racially discriminatory and unjustifiably invasive surveillance tactics of the NYPD, including its surveillance of Muslim communities through the use of license plate readers (LPRs) and other technologies. Despite the passage of the POST Act, the NYPD continues to evade transparency requirements and provide misleading or incomplete information about its surveillance practices. The proposed amendments—Introduction (Int.) 168, Int. 233, and Int. 480—are critical to ensuring that the NYPD is held accountable for its widespread surveillance operations. However, true oversight must also include stronger enforcement mechanisms, such as court review, to prevent continued abuse.

The NYPD has repeatedly demonstrated that it cannot be trusted to ensure its own adherence to the Constitution or to New York State and city laws. This is evident in its chronic noncompliance with other accountability and reform measures, most notably its racially discriminatory street stops, which were the subject of the *Floyd v. City of New York* litigation and ongoing federal monitoring.

As we enter the era of digital stop-and-frisk, the rights and dignity of New Yorkers are at stake. City Council must act now to strengthen the POST Act and implement other meaningful limits

---

[1] *Carpenter v. United States*, 138 S. Ct. 2206, 2213–14 (2018) ("Although no single rubric definitively resolves which expectations of privacy are entitled to protection, the analysis is informed by historical understandings of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted. On this score, our cases have recognized some basic guideposts. First, that the Amendment seeks to secure the privacies of life against arbitrary power. Second, and relatedly, that a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance."

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

on NYPD surveillance to prevent further exacerbation of the department's already highly discriminatory practices.

Despite minor improvements, the NYPD's IUPs lack critical information on both the privacy and legal implications of their Surveillance Technologies

The NYPD has continually failed to comply with both the letter and the spirit of the POST Act, using broad and misleading interpretations to minimize transparency. Rather than fully disclosing the capabilities and implications of its surveillance technologies, the Department selectively omits key details regarding the most critical privacy concerns for New Yorkers.

As highlighted in the OIG's most recent report on POST Act compliance, the Unmanned Aerial Systems (UAS) IUP omits any mention of drones equipped with window-breaking technology and thermographic imaging capabilities, two technologies which raise major Fourth Amendment concerns.[3] The use of such technologies could facilitate unconstitutional warrantless imaging or entry into private residences, violating individuals' reasonable expectation of privacy as protected by the Fourth Amendment.[4] This is exactly the kind of critical information the POST Act is intended to make transparent.

Most IUPs Rules, Processes, and Guidelines sections have extremely basic boilerplate language such as the technology being used "in a manner consistent with the Constitution," without specifying concrete legal standards or limitations.[5] The fact that a practice may be Constitutional is not sufficient information to understand the wide-reaching privacy implications of said practice. For instance, the DAS IUP does not reveal to the public that DAS is used to compile entity reports on individuals, and therefore further does not inform the public as to the criteria for inclusion in the DAS. While a data dragnet that compiles information about citizens may meet some threshold of constitutionality, that does not mean it is not unduly invasive. To illustrate, through our direct client representation, BDS recently learned of an entity report in the DAS for a 5 year old child. This means that the personal information of a kindergartner, including photos and addresses, is available to any number of NYPD's 55,000 employees without any oversight whatsoever over this access. NYPD should be required to publish the criteria for the creation of an entity report—which is essentially a digital dossier—on an individual, as the current lack of transparency allows for the unchecked accumulation of personal data, including that of young children, without any public accountability or oversight.

---

[3] N.Y.C. Dep't of Investigation, DOI Report on the POST Act Release #49-2024 (Dec. 18, 2024), https://www.nyc.gov/assets/doi/reports/pdf/2024/49PostActRelease.Rpt.12.18.2024.pdf.

[4] *See Id.* "the [IUP] makes no mention of this capability of certain UAS to break into a windowed structure in furtherance of this purpose. This capability allows a UAS to gain access to otherwise inaccessible areas, without obtaining a search warrant (on the basis of exigent circumstances, a legal exception to the search warrant requirement), and enables NYPD to conduct surveillance distinct from what would be visible from the naked eye. As such, the UAS IUP should be updated to disclose this capability.

[5] New York City Police Department, *Domain Awareness System (DAS) Impact and Use Policy* 4 (Apr. 9, 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

Additionally, while the DAS IUP notes that DAS itself does not use "biometric measuring technologies," DAS *has* been known to record whether the NYPD has an individual's DNA profile in their DAS entry.[6] To the extent that the NYPD has publicly discussed aspects of this technology, it has focused on the network of CCTV cameras and the Real-Time Crime Center, not on the fact that the DAS is potentially facilitating access to individuals' DNA profiles in defiance of the state law that requires all DNA profiles be stored and accessed in the state-level DNA databank.[7]

Another example is the Digital Forensic Access Tools (DFAT) IUP, which does not specify what forensic tools the NYPD possesses. Instead, the IUP speaks in broad generalizations regarding the department's various DFATs and obscures their particular capabilities. For instance, the IUP fails to mention that NYPD has a contract with GrayKey, a tool capable of brute-forcing its way into encrypted phones.[8] The IUP falsely claims that "the NYPD does not use digital forensic access tools to engage in unauthorized access or hacking,"[9] despite the fact that this is precisely what GrayKey enables.

Moreover, the IUP does not define what constitutes valid consent when an individual provides access to their device. This omission is critical when considering another DFAT the NYPD has in its arsenal, Cellebrite (which was also not specifically named in the IUP). Cellebrite's software is capable of extracting the entire contents of a phone, including metadata, call logs, and app data, yet the public remains uninformed about PD's use of this software because it is not named in the IUP.

Taken together, the omission of these two pieces of information- the lack of standards for a consent search of a technological device, as well as the use of unnecessarily invasive Cellebrite extraction software, obscures a constitutionally questionable NYPD surveillance and investigation practice. As an example, our office has seen NYPD officers coerce minors into handing over passwords under false pretenses, such as claiming they need to call a parent. Once the phone is unlocked, officers then conduct full forensic extractions, violating privacy rights and due process. Individuals subjected to these searches, minors or otherwise, are not informed of the full scope of data being extracted, making it impossible for them to provide truly informed consent.

Other IUPS similarly contain outright falsehoods, such as the cell site simulator IUP. It claims that "[c]ell-site simulators also do not capture emails, texts, contact lists, images or any other data from the device, nor do they provide subscriber account information (for example, an

---

[6] *Id.*

[7] *See* N.Y. Exec. Law § 995-C(6), requiring that DNA records collected for inclusion in the databank be kept within the state system and made available only to designated entities for *specific* law enforcement purposes.

[8] *See* Upturn**,** *Mass Extraction: The Widespread Power of Police to Search Mobile Phones (2020),* https://www.upturn.org/work/mass-extraction/ for an explanation of Graykey's capabilities.

[9] New York City Police Department, *Digital Forensic Access Tools Impact and Use Policy* 3 (Apr. 9, 2021), https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/digital-forensic-accesst-tools-nypd-impact-and-use-policy_4.9.21_final.pdf

account holder's name, address, or telephone number)" - this is incorrect.[10] Both the called and calling numbers are accessible to a cell-site simulator, because this information is also available to any traditional cell tower responsible for routing the communication. Additionally, the IUP claims that "the NYPD cannot record, store, or retain any of the data processed [sic] cell-site simulators." This is also incorrect. A cell-site simulator device produced by Gladiator Forensics and used pursuant to a search warrant records a log of every communication to and from a device it targets. If they have the ability to turn this log over on discovery, they clearly have the ability to record, store, and retain the data processed by a cell-site simulator.

Finally, the Data Analysis Tools IUP is one of the most serious examples of how vague and overly broad categories can be used to prevent the public from understanding the breadth of the techniques used by the NYPD and the depth of the data sources they can draw from. This IUP is written broadly enough to cover almost any AI or machine learning tool the NYPD could deploy, yet gives only a single example of how these tools may be used to characterize this incredibly broad category: "NYPD personnel can visualize assault complaints under investigation within a particular geographic area and identify potential links between investigations using data analysis tools."

The IUP says very little about how such "potential links" are established. It could be anything among the following examples:

- "Hot spot" analysis and predictive policing that attempts to predict where crimes will occur in the future based on historical trends
- Computer vision tools that attempt to automatically classify video footage and assign labels to it, like "individual wearing a red shirt"
- Automated pattern recognition and search capabilities that allow investigators to look for words and terms that recur across seemingly disparate cases, or set up alerts for individuals or cars matching a specific description.
- Dashboards and other data displays about recent incidents in the Real-Time Crime Center.

These are just a few examples, but already give far greater specificity than the NYPD has in its disclosure. The term "Data Analysis Tool" is so broad that the NYPD could use any of the massive datasets under its control to train and deploy an AI system without disclosing its use to the public, because it would meet the technical definition of "Data Analysis Tools." Or it might mean using a language model like ChatGPT to provide a "natural language" interface to data stored in systems like the Domain Awareness System. As we know, new and untested technologies pose risks to the public when they make errors. The public should not learn about the departments' use of untested and unreliable chatbots only when the system hallucinates, or produces incorrect information about, someone's criminal history. To protect New Yorkers from unchecked and potentially dangerous surveillance expansion, NYPD should explicitly name the

[10] New York City Police Department, Cell-Site Simulators: Impact and Use Policy (Apr. 9, 2021), https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/cell-site-simulators-nypd-Impact-and-use-policy_4.9.21_final.pdf.

data analysis tools they use, disclose how these tools process and interpret data, and provide clear policies on oversight and accountability.

City Council must pass Int. 168, 233, and 480 to protect New Yorkers' civil rights and ensure proper enforcement of the POST Act

We commend the City Council for introducing Ints. 168, 233, and 480, which would make crucial strides toward increasing transparency and oversight of the NYPD's use of surveillance technologies. However, we urge the Council to further strengthen these bills to ensure real transparency and reduce the ongoing and future constitutional harms that flow from an unchecked surveillance policing apparatus.

With respect to Int. 168, as previously discussed the NYPD relies on the same boilerplate retention policy across all of its IUPs, failing to provide meaningful details on how long data obtained through distinct technologies is stored, who has access to it, and how it may be shared. We call on the City Council to explicitly require technology-specific retention policies that provide the public with a clear understanding of how their data is handled.

Additionally, as written, Int. 168 requires the NYPD to provide an itemized list of its surveillance technologies only upon request by the Commissioner of Investigation. This places the burden of oversight on an external agency rather than requiring proactive transparency from the NYPD. Instead, the Council should mandate that the NYPD publish an itemized list of all surveillance technologies in use, ensuring ongoing public awareness and scrutiny of its ever-expanding surveillance apparatus.

Like Int. 168, 233 takes a critical step in requiring the NYPD to establish clear policies on the use of facial recognition technology. However, we urge the Council to go further by mandating that the NYPD evaluate its AI tools for racial bias. Studies have repeatedly shown that facial recognition technology disproportionately misidentifies people of color, increasing the risk of wrongful surveillance and false arrests.

The racial bias in facial recognition technology stems from the datasets used to train these AI systems. Many of these datasets are overwhelmingly composed of images of white individuals, making the software significantly less accurate when identifying people of color. A 2019 study by the National Institute of Standards and Technology found that facial recognition algorithms falsely identified Black and Asian faces up to 100 times more often than white faces.[11]

[11] P. Jonathon Phillips et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NIST Interagency/Internal Report (NISTIR) 8280 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

Many police departments treat AI-generated matches as definitive evidence, even when internal policies warn that the results should not be the sole basis for an arrest.[12] In several cases, law enforcement skipped critical investigative steps, ignoring alibis and even DNA evidence that contradicted AI results. Without strict oversight and requirements for independent verification, the NYPD risks using flawed technology to justify arrests, further entrenching racial disparities in the criminal legal system. The City Council must act decisively to ensure that any use of facial recognition technology is subject to rigorous bias evaluations and independent corroboration before being used to detain or prosecute individuals.

Finally, BDS supports the passage of Int. 480, a necessary step in requiring the NYPD to disclose external entities that receive its surveillance data. With that said, the language of Int. 480 can be expanded and clarified to encourage more effective transparency and compliance from the NYPD. As written, Int. 480 only mandates disclosure of who receives NYPD data, but it should also require the NYPD to list every agency and entity from which it obtains data, such as the Department of Corrections (DOC), Department of Education (DOE) and the Office of the Chief Medical Examiner (OCME). Without this full accounting, the public remains unaware of how data flows between agencies, limiting oversight and accountability.

The bill should explicitly mandate that the NYPD identify each external entity by name, detailing both the type of data exchanged and how it is gathered. For example, while the DAS IUP claims that no biometric data is included, DAS reports indicate whether an individual's DNA is on file (whether with OCME or via other systems), proving that biometric data is indirectly linked to NYPD surveillance. This lack of transparency undermines public trust and prevents an accurate assessment of NYPD data-sharing practices.

Additionally, the City Council and the Office of Inspector General (OIG) must ensure the NYPD publishes IUPs for all surveillance technologies they can access, even if those technologies are operated by external entities like the DOC or the Department of Homeland Security. Several significant tools, including Securus, THREADS, and OMNY, remain undisclosed in IUPs despite their widespread use. THREADS, for example, allows correctional staff to analyze the social networks of incarcerated individuals and create maps of individuals' social networks in and out of prisons. Individuals calling their incarcerated family members may have the data from their calls shared with the NYPD, raising the risk that they will be surveilled by the NYPD in violation of both their right to privacy as well as their First Amendment association rights. NYPD staff also have access to federal surveillance systems; excluding them from the authority of the POST Act poses the risk that the NYPD can shield their practices from scrutiny by relying upon third-party sources of surveillance data. The NYPD must be required to produce a full, itemized list of all surveillance technologies in use to prevent selective disclosure and concealment of critical information.

[12] Drew Harwell, *Police Embrace AI and Facial Recognition, Stirring Privacy Concerns*, Wash. Post (Feb. 14, 2025), https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/.

Brooklyn Defenders

City Council Must Close the Loophole and Require Real Transparency on the Disparate Impact of NYPD Surveillance Technologies

Finally, we urge the City Council to amend the POST Act to explicitly require the NYPD to report on the actual disparate impact of the surveillance technologies they use, rather than limiting disclosures to the theoretical impact of written policies. This distinction is critical. The public deserves transparency regarding how these tools function in practice, who is being affected, and whether they are effective in achieving their stated goals.[13]

In past POST Act audits, the Office of the Inspector General (OIG) has repeatedly recommended that the NYPD disclose the discriminatory effects of its surveillance tools.[14] However, the NYPD continues to frame its reporting around the potential disparate impact of its Impact and Use Policies (IUPs) rather than the actual consequences of the technologies themselves. This reporting failure shields the NYPD from accountability and allows ineffective and racially discriminatory technologies to remain in use.

The ShotSpotter IUP contrasted with data on the efficacy of the technology itself exemplifies why disparate impact reporting is crucial to maintaining transparency and ensuring the efficacy of surveillance tools. The NYPD claims that it does not control sensor placement, stating that ShotSpotter engineers determine locations based on gunshot data.[15] Even if this were true, the data itself is unreliable, rendering this justification meaningless. ShotSpotter's confirmation rate—the percentage of alerts verified as actual gunfire—is only 16.57 percent, and over 99 percent of alerts do not result in a firearm recovery or suspect identification.[16] Despite this abysmal performance, the NYPD continues to expand and renew its ShotSpotter contract without public scrutiny. The only reason the public is aware of these failures is due to a FOIL request and subsequent report from our office and an audit from the Comptroller[17], not because of any NYPD disclosure.

---

[13] Currently, the POST Act's disparate impact reporting requirement reads: "any potentially disparate *impacts of the surveillance technology impact and use policy* on any protected groups as defined in the New York City Human Rights Law." *Emphasis added.* N.Y.C. ADMIN. CODE § 14-188(c).

[14] City of New York Department of Investigation, *DOI'S OFFICE OF THE INSPECTOR GENERAL FOR THE NEW YORK CITY POLICE DEPARTMENT ISSUES REPORT ASSESSING NYPD'S COMPLIANCE WITH THE PUBLIC OVERSIGHT OF SURVEILLANCE TECHNOLOGY ACT* (Dec. 2024), https://www.nyc.gov/assets/doi/reports/pdf/2024/49PostActRelease.Rpt.12.18.2024.pdf.

[15] NYC Police Dep't, ShotSpotter - NYPD Impact and Use Policy (Apr. 9, 2021), https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/shotspotter-nypd-impact-and-use-policy_4.9.21_final.pdf.

[16] Brooklyn Defender Services, ShotSpotter: A Systemic Analysis of the Technology's Impact on Communities (Dec. 2024), https://bds.org/assets/files/Brooklyn-Defenders-ShotSpotter-Report.pdf.

[17] New York City 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* (Jun. 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/.

The problem is not just that ShotSpotter is ineffective. Its failures actively harm communities of color. The majority of ShotSpotter sensors in New York are placed in Black and Latine neighborhoods, meaning every time an alert is triggered—even if it is just a car backfiring—it gives officers a justification to enter these areas on high alert, often with guns drawn.[18] ShotSpotter alerts are also used to justify stopping, questioning, and frisking individuals in the vicinity, even when there is no evidence of a crime. Because of its disproportionate placement in neighborhoods with primarily Black and Latine populations, people of color disproportionately bear the burden of these unnecessary and often dangerous police encounters.

Other cities have recognized these risks. Chicago recently canceled its ShotSpotter contract after widespread concerns about its inaccuracy and racialized deployment, which contributed to the fatal police shooting of 13-year-old Adam Toledo, a child killed by officers responding to a ShotSpotter alert.[19] If the NYPD were required to disclose not just policy language but the real-world impact of its surveillance tools, City Council and the public could evaluate whether ShotSpotter and similar technologies cause more harm than good. Instead, the NYPD has avoided scrutiny, relying on unclear reporting requirements in the POST Act while continuing to deploy surveillance tools that fuel over-policing and racial profiling.

The POST Act is a starting point. To further protect New Yorkers rights, we need better judicial and legislative guardrails

- **Oversight of NYPD Surveillance Must Include Court Review to Ensure Constitutional Use**

City Council's oversight role–pushed forward by the POST Act's passage in 2020–currently stands alone amongst administrative and governmental checks on NYPD surveillance powers. This is so because of NYPD's failure to comply with the minimal restrictions imposed by the courts, the city's contracting and procurement processes, the city's budget choices, and the Office of Inspector General.

When it comes to the NYPD's surveillance programs, the Department does not receive any significant oversight from the courts. In its POST Act responses, the NYPD (perhaps unintentionally) revealed that, among the 36 categories of surveillance technology the Department identified, they only believe that *four* require court approval or oversight. Each of these four (two eavesdropping methods, one location tracking method, and one cell phone data extraction method) have been the subject of Supreme Court Constitutional decisions.[20]

---

[18] Brooklyn Defender Services, *supra* note 16.

[19] Martin Kaste, Chicago Mayor Drops ShotSpotter, A Gunfire Detection System, NPR (Feb. 15, 2024), https://www.npr.org/2024/02/15/1231394334/shotspotter-gunfire-detection-chicago-mayor-dropping.

[20] See Katz v. United States, 389 U.S. 347 (1967) (overturning Olmstead v. United States and holding that wiretapping, even in the absence of a physical trespass, requires a warrant); United States v. Jones, 565 U.S. 400 (2012) (holding that location tracking with a GPS device requires a warrant); and Riley v. California, 573 U.S. 373 (2014) (holding that searching and seizing the digital contents of a cell phone requires a warrant).

According to the NYPD, every other surveillance method can be deployed without any court approval or oversight.

This lack of oversight extends to warrantless seizures and searches of cell phones, a critical issue in the context of NYPD's unchecked data-gathering practices. Given the NYPD's extensive surveillance capabilities and troubling testimony from cell phone owners about the state of their devices after police seizures, there is ample reason to believe that the department is exploiting its power to seize property without a warrant as a tool for unauthorized intelligence gathering. In fact, through reviewing NYPD property vouchers for our clients' cell phones, BDS discovered that officers were entering our clients' IMEI numbers into their property tracking system. The IMEI on a phone is essentially a digital serial number which, on most models of the iPhone, can only be accessed by unlocking the phone and entering its Settings. Civil rights advocates have long worried that the NYPD records IMEI numbers in order to track individuals' movement and social media activity.[21] Worse yet, because IMEI numbers can only be accessed through unlocking most phones, simply harvesting the IMEI numbers via a search without a warrant or consent patently violates the legal precedent set in *Riley v. California*.[22] The practice of conducting IMEI searches without a warrant further underscores the need for better oversight and control over the NYPD's power to seize and retain cell phones—once a phone is unlocked, there is little to stop the NYPD from accessing far more data than what is related to the immediate investigation. The expansion of the NYPD's surveillance apparatus, coupled with its willingness to bypass legal protocols, highlights the urgent need for court oversight and clearer guidelines on the retention and use of civilian data. Citizens' devices must not be treated as indefinite sources of intelligence, and the NYPD must provide transparent and lawful justifications for retaining such devices, particularly when investigations or criminal cases have already concluded.

- **Legislative Protection for Civilian Data**

In addition to requiring warrants that reflect current technological capabilities, we must enact stronger data protection laws to safeguard citizens' privacy. The NYPD must face stricter limits on the duration of data retention and be held accountable for how this data is used, ensuring that information is not misused or stored indefinitely without due process. Civilian privacy and constitutional rights should never be secondary to the unchecked power of law enforcement.

Data should be protected similarly to DNA, as both contain highly sensitive, identifying information. New York Executive Law §995-c, which governs the state's DNA identification index, provides a framework for how sensitive data should be handled, setting important precedents for data privacy, retention, and sharing. For instance, DNA records are only released

---

[21] Graham Rayman, *NYPD seeks to grab cell phone IDs from people under arrest or in custody; push for IMEI numbers raises concerns*, Daily News. https://www.nydailynews.com/2023/07/08/nypd-seeks-to-grab-cell-phone-ids-from-people-under-arrest-or-in-custody-push-for-imei-numbers-raises-concerns/.

[22] *See Riley v. California*, 573 U.S. 373 (2014), holding held that police must obtain a warrant before searching digital information on a cellphone seized from an arrestee, as the search-incident-to-arrest exception does not apply to modern cellphones due to their vast storage capacity and the privacy concerns involved.

under strictly defined circumstances, such as to law enforcement agencies through written agreements or to defendants for their legal defense. Civilian data collected through surveillance technologies should be subject to similar constraints to prevent indiscriminate sharing and misuse.

Furthermore, Executive Law §995-c includes provisions for data expungement, ensuring that DNA records are removed when convictions are overturned or charges are dropped. A similar mechanism must be established for digital data collected by the NYPD, allowing individuals to request the deletion of their personal information if it was gathered without legal justification or if the associated case does not result in prosecution. Without such safeguards, New Yorkers face indefinite retention of their personal data with little recourse.

Conclusion

The NYPD has demonstrated time and again that it will resist transparency measures unless forced to comply. Without aggressive enforcement, enhanced legislative protections, and court oversight, the Department will continue to expand its unchecked surveillance power, deepening existing inequities in policing and eroding fundamental civil liberties.

As Professor Andrew Ferguson noted before the United States Congress in 2019, "the Fourth Amendment will not save us from the privacy threat posed by [surveillance] technolog[ies]. The Supreme Court is making solid strides in trying to update Fourth Amendment principles in the face of new technology, but they are chasing an accelerating train and will not catch up. Legislation is needed to respond to the real-time threats of real-time technology."[23] The burden now falls on legislative bodies, including the City Council, to enact meaningful reforms before these technologies become even further embedded in the daily lives of New Yorkers.

Unchecked surveillance does not equate to safety. It increases government overreach, fuels discriminatory policing, and diminishes the freedoms of those who already face systemic oppression. The City Council must act now to close loopholes, impose stricter oversight, and ensure that the POST Act is a meaningful tool for accountability. We urge the Council to pass Int. 168, 233, and 480, implement additional protections against surveillance abuses, and hold the NYPD accountable to the communities it is meant to serve.

If you have any questions, please do not hesitate to contact Jackie Gosdigian, Senior Policy Counsel, at jgosdigan@bds.org.

[23] Andrew Guthrie Ferguson, "Written Testimony of Professor Andrew Guthrie Ferguson before the House of Representatives Committee on Oversight and Reform," Hearing on Facial Recognition Technology: Its Impact on our Civil Rights and Liberties (May 22, 2019).