STATEMENT OF
ALBERT FOX CAHN, ESQ.
EXECUTIVE DIRECTOR
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT, INC.*

BEFORE THE
COMMITTEE ON PUBLIC SAFETY
NEW YORK CITY COUNCIL

SUPPORTING
INT 0635-2018 AND T2018-2223

PRESENTED
June 27, 2019

* My sincerest thanks to S.T.O.P. Civil Rights Interns Ayyan Zubair and James Blum for their invaluable assistance in preparing these remarks.
Good morning, my name is Albert Fox Cahn, and I serve as the Executive Director for the Surveillance Technology Oversight Project (“STOP”). STOP advocates and litigates for New Yorkers’ privacy, fighting discriminatory surveillance. I commend the committee and Chairman Richards for today’s hearing; for bringing much-needed attention to the injustice and discrimination fueled by the NYPD’s gang database and “perp-walks.”

I speak in support of both T2223 and Introduction 635; both measures are important steps to protect New Yorkers’ privacy. But I also testify more broadly about the current privacy threats to New Yorkers, many of which will require additional legislation.

**T2223 – Gang Database**

For decades, the NYPD’s discriminatory “Stop and Frisk” policy racially profiled New Yorkers of color, stripping them of their most fundamental rights because of the color of their skin. While New York has largely curtailed that unconstitutional blight, we continue to maintain police policies that subject New Yorkers of color to invasive, unjustified, and dehumanizing surveillance. One of the most disturbing systems is the “gang database.”

Let’s be clear, the NYPD’s gang database is little better than high-tech “Stop and Frisk.” Rather than stopping racial profiling, the NYPD simply shifted from physical pat-downs to electronic searches—adding eleven New Yorkers to their sprawling database every single day. The gang database treats New Yorkers as criminals just for how they dress and where they live. Children and teenagers report that the constant surveillance is so traumatic that they are sometimes afraid to leave their homes and socialize with their friends, terrified of falsely being labeled as a “gang member.” T2223 is the first step towards correcting this injustice and creating a more equitable criminal justice system in New York City.

It’s hard to understand how the NYPD still defends their discriminatory database. The definition of “gang” should include everyone from the mafia to white supremacists, but the database remains ninety-nine percent New Yorkers of color. When you look at how the database is actually compiled, this discrepancy is no surprise. Leaked NYPD training documents show officers trained to systematically profile people of color as “gang affiliated.” The NYPD includes numerous New

---

1 We believe that the term “perp walk” only normalizes the NYPD’s “guilty until proven innocent” framing. However, the term is used throughout as to avoid potential confusion.


Yorkers simply for wearing a suspicious color of clothing or just being in the same neighborhood as a suspect.⁶

To end this abuse, we need transparency, but we also need more. Even as we applaud Chair Richards’ introduction, we don’t believe it goes far enough. Yes, New Yorkers must know when they’ve been caught-up in the NYPD’s Surveillance dragnet, but they also need the tools to cut themselves free. Being labeled a “gang member” is no small problem. The label leads to increased surveillance, criminal and immigration consequences, and lasts for at least three years—often indefinitely. Such a label should not be beyond redress for any New Yorkers.

Giving minors the power to contest inclusion in the database is a crucial first step in protecting our most vulnerable communities. But that right should extend to every single New Yorker who is tracked and targeted for the “crime” of their clothing, neighborhood, and skin color. We are encouraged by the committee’s attention, but we urge it and the Council to take on the more systemic reforms needed to end this type of digital discrimination.

Intro 635 – “Perp-Walks”

Today, so-called “perp-walks” give the NYPD the power to demonize and denigrate New Yorkers who have not yet been indicted for, let alone convicted of, any crime. They are an affront to our constitutional system and the indispensable presumption that we are all innocent until proven guilty. Sadly, we know too well that countless New Yorkers, predominantly New Yorkers of color, are arrested for crimes they never committed. While these adults and children may win their case at trial, they’ll never be able to undo the reputational harm from having their photo wrongfully labeled as a “perp.”

These extra-judicial photo ops undermine due process and fundamental fairness. In extreme cases, federal courts have even held “perp-walks” as unconstitutional seizures.⁷ Even when lawful, the practice gives the NYPD tremendous power over New Yorkers, power that the NYPD leverages to coerce suspects and reinforce shameful stereotypes. New Yorkers deserve their day in court, not trial in the court of public opinion. I commend the committee and Council Member Dromm, for pursuing this vital reform.

The POST Act

Both of the foregoing measures speak to the urgent need to protect New Yorkers from warrantless, discriminatory privacy invasions. But as important as these measures are, they only address small segments of New York’s growing privacy threats. The sheer scale of New York’s surveillance requires systematic responses, and no measure is more urgent than the POST Act. The Public Oversight of Surveillance Technology (“POST”) Act requires the NYPD to systematically develop privacy protections for each and every spy tool it deploys.⁸

---

⁷ Lauro v. Charles, 219 F.3d 202 (2d Cir. 2000).
The NYPD built up an arsenal of invasive spy tools on the public tab while trying to block any public notice or debate. These tools not only include the Gang Database, but items like facial recognition, surveillance lightbulbs, and automated license plate readers that can monitor a vehicle’s location throughout the city.

These tools pose a privacy threat to all New Yorkers, but they pose a particularly potent threat to our immigrant communities. All too often, these systems create a risk of information sharing with federal agencies—even ICE. For example, the NYPD has contracted for years with the private firm Vigilant Solutions, which operates a nationwide database of over 2 billion license plates data points.\(^9\) Shockingly, last year we learn that that Vigilant Solutions was not just contracting with local police departments—it was also contracting with ICE.\(^10\) This is the vendor that the NYPD uses to record at least one million license plates per day.\(^11\)

Perhaps most disturbingly, the NYPD relies on Vigilant Solution’s artificial intelligence to map out social networks, label New Yorkers as “criminal associates”, and create databases based on the company’s unproven algorithms.\(^12\) This is just one example of countless surveillance tools that requires a systematic solution.

The POST Act is a comprehensive response, but it’s also a modest one. The NYPD can continue using these tools—no matter how problematic—by complying with modest protections against waste, discrimination, and misuse. In fact, the POST Act would be one of the weakest surveillance reform bills in the country.\(^13\) Just compare the bill to San Francisco\(^14\) and Oakland, which banned facial recognition technology,\(^15\) and Massachusetts is even considering a state-wide moratorium on

---


\(^10\) The Domain Awareness System collects the license plate data scanned by the approximately 500 license plate readers operated by the NYPD and combines it with footage from cameras and other surveillance devices around the city. The NYPD holds on to the license plate data for at least five years regardless of whether a car triggers any suspicion. See MARIKO HIROSE, *Documents Uncover NYPD’s Vast License Plate Reader Database*, ACLU, Jan. 25, 2016, https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-reader-database?redirect=blog/speak-freely/documents-uncover-nypds-vast-license-plate-reader-database.

\(^11\) See id.

\(^12\) See id.


facial recognition.¹⁶ The evidence is clear, civilian surveillance oversight enhances public trust in police departments public safety.¹⁷

I’m grateful that the committee is addressing New Yorkers’ myriad privacy concerns. Our alarm grows by the day, as emerging technologies exacerbate the threats we are only now starting to address. I hope that New York City rises to the task before it is too late. We urge this committee to build on the momentum it generates today by reforming the NYPD gang database and so-called “perp walks” by taking up the next, crucial task of passing the POST Act.


¹⁷ Oakland, California and Seattle, Washington have enacted similar police oversight laws without deteriorating public safety. See id.