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

BEFORE THE
COMMITTEE ON TECHNOLOGY
&
COMMITTEE ON HOUSING AND BUILDINGS
&
COMMITTEE ON CONSUMER AFFAIRS AND BUSINESS LICENSING
NEW YORK CITY COUNCIL

FOR A HEARING CONCERNING,
USE OF BIOMETRIC TECHNOLOGY ON RESIDENTIAL AND COMMERCIAL ESTABLISHMENTS.

SUBMITTED
October 7, 2019
Good morning, my name is Albert Fox Cahn, and I serve as the Executive Director for the Surveillance Technology Oversight Project (“S.T.O.P.”). S.T.O.P. advocates and litigates for New Yorkers’ privacy, fighting discriminatory surveillance. I commend the committees for today’s hearing and for protecting New Yorkers from the unrestricted collection of their biometric data.

I speak today in support of both the KEYS Act and Introduction 1170 as important first steps to protect New Yorkers’ privacy, but I would also like to voice my concerns over the potential unintended consequences of Introduction 1672. Additionally, I will speak to the need to go much further in our efforts to protect New Yorkers from biometric data collection and other threats to our privacy.

T2019-4579 – the Keep Entry to Your home Surveillance-free “KEYS” Act

The Keys Act is a helpful response to concerns over landlords’ collection of tenant biometric data and other forms of residential surveillance. S.T.O.P. supports this measure and the principle that no New Yorker should be forced to let their landlord track their every movement just to get a roof over their head.

Last fall, tenants of Atlantic Plaza Towers, a rent-stabilized apartment complex in Brooklyn, were alarmed to learn of plans to replace their buildings’ key-fob systems with facial recognition. Tenants refused to indefinitely surrender their biometric data for a system with no clear benefit. Atlantic Plaza already has 24-hour security, including both cameras and guards. Adding facial recognition on top of these existing systems will only harm tenants, especially given facial recognition’s documented bias against communities of color, particularly black women.

M.I.T. and Stanford researchers have documented commercial facial recognition systems’ systemic discrimination. Many of these systems are incredibly accurate for Caucasian men under certain test conditions, but they fail up to one-third of the time for Black women in those same exact condition. Facial recognition systems have similarly been shown to perform poorly on the elderly and children.

The harmful consequences of over-surveillance are well-documented, as is the fact that communities of color disproportionately suffer from its adverse effects. Complexes like Atlantic Towers already over-surveil their residents. Tenants report receiving warnings and fines for issues as minor as where they walk their dog and what appliances they purchase, all as a result of existing CCTV Surveillance.

---

The privacy impact of biometric surveillance will be far more extreme than CCTV. Existing laws fail to limit a landlord’s ability to retain and resell biometric data from tenants, even years after their lease expires. More expansive surveillance will raise concerns about coercion in eviction cases to outright blackmail. Even worse, Landlords will be required to provide biometric data if subpoenaed by a government agency, including U.S. Immigration and Customs Enforcement (I.C.E.).

These concerns have inspired proposals for state-wide and federal bans on landlords’ use of facial recognition. Importantly, the KEYS Act goes further in some ways and also protects against the data tracking capability of electronic key fobs, which are already in widespread use. However, the bill does not offer tenants complete privacy. While a tenant may be able to opt-out of using facial recognition to access the building, that won’t prevent their face from being recorded and potentially logged dozens or even hundreds of times a day. While an opt-out is completely appropriate for systems like key fobs, we must follow the lead of other jurisdictions that have begun to ban facial recognition outright.

Intro 1170-2018

As biometric surveillance becomes cheaper and more prolific, New Yorkers will face a city where every purchase, conversation, and movement will be recorded and stored. The surveillance city creates a detailed record of life, not only available to the companies tracking our every movement, but also potentially government agencies like I.C.E. and even hackers.

Introduction 1170 is an important step in stemming the surveillance tide that threatens to drown out our most basic liberties. New York businesses already capture our biometric data, including images, video, or audio recordings. Current laws allow biometric data not only without our consent, but without even our knowledge. Commercial firms don’t tell us how we’re being recorded on the way to the subway, picking up our morning coffee, or even walking into a doctor’s office.

While it will be helpful to have public notice of biometric surveillance as required by intro 1170, it’s not an adequate solution. It’s an improvement to require storeowners to give the public notice, but we need to go even further and ban this sort of biometric tracking completely. We are quite concerned that such public notices will be particularly ineffective for non-native English speakers, compounding their risk of biometric tracking.

Intro 1672-2019

Introduction 1672 requires the creation of a city-run biometric surveillance database, recording the location of any private firm using such technology. Though well-intentioned, this database could exacerbate the threat posed to the public by biometric surveillance. The database could provide hackers with what amounts to a target list, identifying the firms that hold our biometric data.
One of the most basic cybersecurity protections is “security through obscurity.” Attackers can’t target your data if they don’t know you have it. Right now, the lack of a centralized biometric database makes it more difficult for hackers to know whom to target, a safeguard we would lose with Intro 1672. Similarly, this database could easily be used by local, state, and federal law enforcement, including I.C.E., to find private surveillance systems that could be co-opted for criminal and immigration enforcement purposes.

Regrettably, the bill would fail to remedy the most glaring problems with biometric surveillance. The bill does not require landlords to disclose the details that a tenant would need to truly understand how a surveillance system operates. This includes what data is collected, how it is collected, with whom and under what circumstances it is shared, and if the landlord is compensated by the vendor. Even if the bill required adequate disclosure, it would still fail to require landlords to obtain informed consent from their tenants, never mind guests, delivery people, and others whose biometric information is captured. Lastly, the bill fails to restrict landlord’s ability to retain or sell data.

The POST Act

The foregoing measures are well-intentioned, but, regrettably, they fall short of creating the comprehensive privacy protections New Yorkers need. Most disturbingly, they highlight the city’s failure to address its own sprawling biometric surveillance apparatus. For more than two years, I’ve fought for enactment of the only bill to comprehensively regulate The New York City Police Department (“NYPD”) surveillance regime: The Public Oversight of Surveillance Technology (“POST”) Act.5

For years, the NYPDs acquired an arsenal of invasive spy tools on the public’s dime, while thwarting any public disclosure or debate. These tools include items like facial recognition, surveillance lightbulbs, and automated license plate readers that can monitor a vehicle’s location throughout the city. Facial recognition alone has led to the arrests of thousands of New Yorkers, many wrongly accused.

These tools pose a privacy threat to all of us, but they pose a particularly potent threat to members of our immigrant communities. All too often, these systems create a risk of information-sharing with federal agencies, including ICE. For example, the NYPD for years has contracted with the private firm Vigilant Solutions, which operates a nationwide database of over two billion license-plate data points.6 Shockingly, in 2016 we learned that Vigilant Solutions was not just contracting with local

police departments but also with ICE.7 This is the vendor the NYPD uses to record at least one million license plates each day.8

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.9

The POST Act is not just a comprehensive response, but also a modest one. The NYPD can continue using these tools—no matter how problematic—by complying with limited protections against waste, discrimination, and misuse. In fact, the POST Act would be one of the weakest surveillance reform bills in the country,10 especially when viewed in comparison to San Francisco’s11 and Oakland's outright bans on facial recognition technology12 and Massachusetts's state-wide moratorium.13

The evidence is clear: civilian oversight of surveillance enhances the public’s trust in police departments and public safety.14 Now, with twenty-eight city council members signed on as POST Act cosponsors, the time is long overdue for a hearing before the public safety committee and a vote of the full council.

I hope that New York City rises to this challenge before it is too late. We urge the Council to build on the momentum it generates today by making passage of the POST Act a top priority.

---

7 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-readerdatabase?redirect=blog/speak-freely/documents-uncover-nypds-vast-license-plate-reader-database.
8 See id.
9 See id
14 Oakland, California and Seattle, Washington have enacted similar police oversight laws without deteriorating public safety. See id.