Testimony of Steven Ettannani
New York City Department of Consumer Affairs

Before the
Joint Committee of Technology, Housing & Buildings, and
Consumer Affairs & Business Licensing

Hearing on
Int. No. 1170-2018

October 7, 2019

Good morning Chairs Holden, Cornegy Jr., Espinal and members of the joint committee. My name is Steven Ettannani and I am the Executive Director for External Affairs at the New York City Department of Consumer Affairs, recently renamed the Department of Consumer and Worker Protection (DCWP). I would like to thank the joint committee for the opportunity to testify today on behalf of DCWP Commissioner Lorelei Salas regarding Int. 1170 related to requiring commercial establishments to notify customers of their use of biometric identifier technology. DCWP appreciates and shares the Council's concern regarding the collection of biometric information and consumer privacy.

DCWP protects and enhances the daily economic lives of New Yorkers to create thriving communities. DCWP licenses more than 75,000 businesses in more than 50 industries and enforces key consumer protection, licensing, and workplace laws that apply to countless more. By supporting businesses through equitable enforcement and access to resources and, by helping to resolve complaints, DCWP protects the marketplace from predatory practices and strives to create a culture of compliance. Through our community outreach and the work of our Offices of Financial Empowerment and Labor Policy & Standards, DCWP empowers consumers and working families by providing tools and resources they need to be educated consumers and to achieve financial health and work-life balance.

In today's marketplace, the use of technology to connect to the services and products we utilize is ubiquitous. Advances in technology now make it possible for consumers to use their biometric information for purposes of identification or authentication on networking platforms, devices, and more. Increasingly, biometric information is replacing traditional forms of access control, such passwords and pins[1].

At the same time, we are becoming aware of the unique challenges presented by the embedding of this technology into our everyday devices and how it facilitates the collection of biometric information by businesses and third parties. For example, multinational companies have long applied their access to consumer photos and videos to develop facial recognition technology[3]. What once seemed innocuous and convenient has now raised legitimate questions of the need for consumer consent and control over the collection, use, and sharing of biometric information. This is even more salient with the potential for large-scale breaches of databases containing

[1] https://venturebeat.com/2019/09/29/its-not-too-late-to-get-biometrics-right/

consumer biometric information[2]. Due to these concerns, we have seen states across the country, such as Montana, Florida, and even New York develop legislation to prohibit the collection of biometric data without consumer consent.

Consumer protection is at the heart of DCWP's mission; and a myriad of laws guide our work toward the fundamental principle that an educated consumer is best positioned to make informed decisions in the marketplace. Naturally, a part of consumer education includes requiring businesses to post conspicuous notices and disclosures. DCWP requires signage related to price posting, refund policies, and consumer rights pursuant to various City, and State laws depending on the business. To promote compliance, DCWP regularly educates individual businesses and trade associations about their legal obligations.

Int. 1170 requires commercial establishments, defined as "any premises exercising trade, business, profession, vocation, commercial or charitable activity," across the City to conspicuously post signage alerting consumers that the establishment is collecting their biometric identifier information. This information could include, a retina or iris scan, fingerprints, voiceprints, hand scan, or "face geometry." Additionally, these establishments would have to make available online a description of the type of information they are collecting, how long it is being collected for, who they share the information with, and the establishment's overall privacy policy governing the collection of the biometric information. DCWP supports the intent of this legislation but has concerns with enforcement of its provisions as currently drafted.

First, the scope of "biometric identifier information" is unclear. For example, does a security camera capture an individual's "face geometry"? If so, does it matter whether the footage was "collected" to "identify an individual"? Absent guidance, the scope of conduct covered by the bill is ambiguous. Second, DCWP's typical enforcement practice, with respect to signage requirements, is for inspectors to conduct onsite inspections to verify that the signage has been posted. But, before issuing a violation, DCWP would need reason to believe that an establishment is collecting, retaining, converting, sorting, or sharing "biometric identifier information." Inspectors in the field will be unable, in most circumstances, to determine whether a business is capturing biometric information, especially if the business is doing so surreptitiously. And, DCWP does not have the investigative expertise to assess whether a business is, for example, collecting "retina or iris scans." Third, Int. 1170's definition of commercial establishment appears to implicate nearly every brick-and-mortar business, or premise conducting charitable activity in New York City. Determining how many of those establishments are collecting "biometric identifier information" and then conducting an onsite inspection and online audit for each establishment poses extraordinary operational challenges. For the above reasons I have outlined, DCWP supports the intent of the legislation but would like to work with the Council and hear from today's panelists about how best to address these enforcement concerns.

As I said earlier, DCWP believes that businesses and consumers alike reap the benefits of a fair and transparent marketplace. The Agency welcomes a frank and thorough discussion about the

[4] https://www.forbes.com/sites/forbestechcouncil/2019/10/04/how-facial-recognition-needs-to-improve-to-be-effective/#7cfcfa332cdf

scope of biometric information collection, its prevalence citywide, and how we can empower consumers, through disclosures, to make informed decisions. Thank you for the opportunity to testify today and I am now happy to answer any questions you may have.

Testimony of the New York City Department of Housing Preservation and Development
Regarding Preconsidered Introduction T2019-4579
October 7, 2019

Good morning, Chairs Cornegy, Holden, and Espinal, and members of the Committees on Housing and Buildings, Technology, and Consumer Affairs and Business Licensing. My name is Sarah Mallory and I am the Executive Director of Government Affairs with the New York City Department of Housing Preservation and Development (HPD). Thank you for the opportunity to testify on Preconsidered Introduction T2019-4579 sponsored by Council Member Lander. This bill proposes a modification in the Housing Maintenance and Buildings Codes to clarify that building owners must provide mechanical keys to residents and cannot require the use of only electronic, keyless entry methods.

The de Blasio Administration has made protecting tenants a core part of its strategy to confront the affordable housing crisis. This Administration has worked in partnership with the City Council and various branches of government to tackle the issue with a comprehensive, multi-pronged approach. As a City, we are focused on keeping people in their homes and neighborhoods by successfully advocating with many members of the Council to close loopholes in rent regulation laws at the State level, creating and preserving historic numbers of affordable homes, empowering tenants with more resources, aggressively enforcing City codes, and utilizing all of our partnerships to create data-driven, innovative tools targeted at stopping harassment before it starts.

Physical security is an important part of ensuring that residents feel safe in their homes. Currently, HPD can and does issue violations for building entrance doors and individual unit doors without lock sets in rental buildings, or those with only electronic entry mechanisms. Electronic, keyless entry methods without the option for mechanical keys are concerning for two reasons: 1) dangers posed by being locked out, or locked in, or not being able to lock a door at all if the energy source for the building becomes unavailable, and 2) the potential for electronically tracking the movement of residents. We support maintaining the requirements for manual lock and key sets until electronic methods of entry can be proven to not pose safety or privacy concerns and thank Council Member Lander for his leadership on this issue.

Thank you again for the invitation to testify and for hearing this bill today. I look forward to answering any questions you may have.

NYC DOITT
Information Technology & Telecommunications

DEPARTMENT OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS TESTIMONY BEFORE THE CITY COUNCIL COMMITTEES ON HOUSING AND BUILDINGS; CONSUMER AFFAIRS AND BUSINESS LICENSING; AND TECHNOLOGY

Introduction 1672 By Council Members Richards and Kallos
A Local Law to amend the administrative code of the city of New York, in relation to requiring real property owners to submit registration statements regarding biometric recognition technology utilized on the premises

MONDAY, OCTOBER 7, 2019

Good Morning Chairs Cornegy, Espinal, and Holden, and members of the New York City Council Committees on Housing and Buildings; Consumer Affairs and Business Licensing; and Technology. My name is Robin Levine and I am the Assistant Commissioner for External Affairs and Communications for the Department of Information Technology and Telecommunications, also known as DoITT. I am here today to discuss Introduction 1672, by Council Member Richards, a Local Law to amend the administrative code of the city of New York, in relation to requiring real property owners to submit registration statements regarding biometric recognition technology utilized on the premises.

As many of you are aware, DoITT delivers a wide range of technology services to over 100 City agencies and governmental entities. Much of our public-facing work that you are most familiar with is our franchise portfolio, wherein we execute franchise agreements with telecommunications companies for use of public rights-of-way. While that is important work, our core mission as an agency is to help our sister agencies fulfill their duties to serve New York City's 8.5 million residents through technology. Among our functions for other agencies are: hosting e-mail, managing the Citywide Service desk, negotiating Master Services Agreements, hosting nyc.gov, and maintaining data centers.

To best serve agencies with the resources they need, we regularly touch base with each agency's Chief Information Officer (CIO). An agency's CIO will make policy decisions on the kind of technology support an agency needs, and confers with DoITT accordingly. We do not, and should not, unilaterally make decisions about what technology solutions agencies need to fulfill their policy goals, but we do work closely with each agency to figure out how to best support them.

Thus, DoITT's service model is designed to serve other government agencies, as opposed to real property owners. Introduction 1672 would task DoITT with collecting registration statements from real property owners about the biometric technology they employ, enforce penalties against real property owners for failing to register, and maintain a publicly searchable database of registered properties.

While we appreciate the confidence that the Council has in DoITT to fulfill the proposed requirements in this legislation, we are not the appropriate entity to do so. As written, Introduction 1672 is not about the deployment of technology – it creates a new reporting requirement for real property owners. As such, we do not have existing tracking and enforcement processes that would make this a good fit for DoITT.

Nonetheless, we look forward to working with our sister agencies and the Council on an approach that would make best use of our areas of expertise. For example, the section of the legislation relating to a public-facing database is something we could assist the enforcing agency with building and deploying, according to their specifications based on current data collecting and storing practices.

We applaud the Council's foresight in tackling this emerging area of policy. DoITT has been examining the broader issue of privacy as it relates to our franchisees, and today's discussion is a welcome complement to this work. I'm happy to answer Council Member questions.

###

SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

@ the Urban Justice Center:
40 Rector Street, 9th Floor
New York, New York 10006
www.S.T.O.P.Spying.org | (646) 602-5600

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.[1] Facial recognition systems have similarly been shown to perform poorly on the elderly and children.[2]

The harmful consequences of over-surveillance are well-documented,[3] as is the fact that communities of color disproportionately suffer from its adverse effects.[4] 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.

---

[1] MIT Press, *Study finds gender and skin-type bias in commercial artificial-intelligence systems*, available at https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

[2] Jack Corrigan, *Experts Tell Congress Facial Recognition's Bias Problem May Be Here to Stay,* NextGov, available at https://www.nextgov.com/cio-briefing/2019/07/experts-tell-congress-facial-recognitions-bias-problem-may-be-here-stay/158320/

[3] *See, e.g.*, Carlos Torres et al., *Indiscriminate Power: Racial Profiling and Surveillance Since 9/11*, 18 U. PA. J.L. & SOC. CHANGE 283, 299–300 (2015).

[4] *See, e.g.*, BARTON GELLMAN & SAM ADLER-BELL, CENTURY FOUND., THE DISPARATE IMPACT OF SURVEILLANCE (2017).

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

[5] Public Oversight of Surveillance Technology (POST) Act, Int 0487-2018.
[6] See ROCCO PARASCONDOLA, Exclusive: NYPD will be able to track fugitives who drive past license plate readers across the U.S., N.Y. DAILY NEWS, Mar. 02, 2015, https://www.nydailynews.com/new-york/nypd-track-fugitives-drive-license-plate-readersarticle-1.2133879.

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's[11] and Oakland's outright bans on facial recognition technology[12] 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

[10] See ACLU, Community Control Over Police Surveillance, https://www.aclu.org/issues/privacytechnology/surveillance-technologies/community-control-over-police-surveillance

[11] See CONGER, KATE, San Francisco Bans Facial Recognition Technology, N.Y. TIMES, May 14, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

[12] See EDITORIAL BOARD, San Francisco Banned Facial Recognition. New York Isn't Even Close. N.Y. TIMES, May 18, 2019, https://www.nytimes.com/2019/05/18/opinion/nypd-post-act-surveillance.html.

[13] See MASSACHUSETTS SENATE, Bill S.1385, https://malegislature.gov/Bills/191/S1385.

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

October 7, 2019

Committee on Housing and Buildings
Committee on Technology
Committee on Consumer Affairs and Business Licensing

Vanessa Bergonzoli
vbergonzoli@gmail.com

RE: Key FOB Hearing -- Tenant Statement

I am a member of the Tenants Association ("TA") at 240 Broadway Brooklyn,NY, (the "Building") I call home. I have volunteered to attend this meeting and offer testimony out of great concern for potential violations that the electronic key fob system ("fob") poses to the right to privacy. The Building, where I have lived for almost a decade, was sold earlier this year and a little over a month ago, my neighbors and I received a letter from Livingston Management, (the "management") agent for the new owner and landlord of the Building, indicating their plan, to switch over from a traditional key to a fob system. I am providing a copy of their letter as part of my testimony.

The owner via management, asked for invasive information including a photograph of myself as well as the names, permanent addresses, and photographs of people in connection with my unit who would be receiving an additional fob to enter the building. I do not see why I should have to supply third party private information to my landlord in order to gain access to the building for those who need to enter my home. That is a violation of their privacy and in forcing me to provide it I am made complicit in that violation by the owner and management.

The letter from management stated that their reason for the change from key to fob was "an effort to improve security in the Building and protect the Building and its residents". Meanwhile the owner is currently engaged in proceedings to evict many (and eventually possibly all) of the residents, making their claims about the improvement of security, simply bogus. It's hard to believe they desire to make the building safe for the very residents they want to evict.

A fob itself may seem harmless, but put the fob together with the surveillance cameras that have now been installed in the Building, photographs of residents and their guests

and with the right software it can all turn into a facial recognition system used to track details of a tenant's private life. Why should landlords have access to this level of data on tenants, especially under the guise of collecting such information to improve security, when in reality this same technology may also be used as a tool to monitor and potentially harass tenants?

I was offered no choice. I was offered no information about the fob, nor about the tech companies that run the system with access to my private information and whether they in turn will be providing that information to third, fourth or fifth parties. In order to have a choice in this matter and not without incurring significant costs, our building's TA sought legal representation to challenge the use of fob keys. The outcome is still uncertain. In sharing my experience with you here today my hope is that it be carefully considered by those who can help protect the rights to privacy for all New Yorkers whether they be renters or landlords.

Sincerely,

Vanessa Bergonzoli

Livingston
Management Services

225 West 35th Street, 14th Floor, New York, NY 10001

Phone: (646) 214-0321 Email: mgmt@livingny.com

September 5th 2019

VIA REGULAR MAIL and E-MAIL

Dear Tenants/Occupants:

RE: Installation of New Key Fob System
240 Broadway, Brooklyn, NY

Dear Tenants:

As you are aware, Livingston Management is the managing agent for 240 Broadway Property, LLC, the owner and landlord ("Owner") of 240 Broadway, Brooklyn NY (the "Building").

In an effort to improve security in the Building and protect the Building and its residents, we will be installing a new electronic key fob system (the "Fob System"). We are sending you this letter to inform you that we will be transitioning to the Fob System for the active entrance doors leading directly to the street.

The new Fob System will replace the existing traditional key system and you will need a new electronic key to access the Building (a "Fob"). We will be distributing one (1) Fob to each full-time occupant of the Building. For security purposes, each occupant will be required to provide Owner with a photograph so your identity can be verified in the event a replacement Fob is required.

Owner will also provide a Fob to each household employee, such as a dog walker or cleaning person, at the Tenant's request. In the event an additional Fob is requested for a household employee, Tenant must provide the name, permanent address, and photograph of the household employee who will be receiving the additional Fob. This information will be securely stored by Owner for security purposes.

Additionally, Owner will provide 1 additional Fob ("Guest Fob") per unit to be used for household guests. Guest Fobs will be registered to the Tenant of Record for each unit.

If an occupant vacates, or a household employee no longer works in the household, the Fobs and Guest Fobs provided to those persons shall be returned to Owner within 48 hours of the occupant's vacatur or the household employee no longer being employed.

In the event a replacement Fob is requested for any reason, Owner will charge the person requesting a replacement Fob a $25.00 fee for a replacement.

We expect the Fob System to be live beginning on September 20, 2019. Please provide Owner with the information required in this letter by September 12, 2019(within two weeks) to ensure each full-time occupant and household employee is provided with a Fob in advance of the Fob System's implementation.

Thank you for your cooperation.

Austen Rabbie
Livingston Management

BRENNAN
CENTER
FOR JUSTICE

at New York University School of Law

120 Broadway
Suite 1750
New York, New York 10271
646.292.8310 Fax 212.463.7308
www.brennancenter.org

Written Testimony of Laura Hecht-Felella
Legal Fellow, Liberty & National Security Program
Brennan Center for Justice at NYU School of Law
Before the
Committee on Housing and Buildings, Committee on Technology, and the Committee on Consumer Affairs and Business Licensing
October 7, 2019

Good afternoon members of the Committee on Housing and Buildings, Committee on Technology, and the Committee on Consumer Affairs and Business Licensing.

My name is Laura Hecht-Felella. I am a Legal Fellow with the Liberty and National Security Program at the Brennan Center for Justice.

Thank you Chairman Cornegy, Chairman Holden, and Chairman Espinal for holding this hearing and inviting the Brennan Center to testify.

The Brennan Center is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. The Liberty and National Security Program in particular focuses on ensuring that government use of new technologies does not violate fundamental rights.

The Brennan Center commends the City Council on its commitment to addressing the growing prevalence of biometric identification technology in New York City. However, we must also express our disappointment that this commitment has not resulted in oversight of the New York City Police Department ("NYPD").

Meaningful efforts by the City Council to increase transparency of biometric identification technology in New York City must include the NYPD. The NYPD's expansive arsenal of surveillance technology includes several biometric tools like facial recognition, video analytics, and DNA databases. Attached to my testimony is a chart that the Brennan Center published this morning. It outlines the scope of the NYPD's surveillance capabilities, referencing documents obtained in Freedom of Information Law litigation and other publicly available information. Our chart identifies several technologies for which the NYPD has failed to provide even basic information about its policies. For many of its biometric tools, like facial recognition, the NYPD has failed to identify whether it has effective safeguards in place to protect New Yorkers' civil rights and privacy.

Biometric identification technology works by using algorithms to try and identify a person based on distinctive physical or behavioral characteristics.[1] Examples of these characteristics include someone's fingerprints, DNA, face, gait, or voice.[2]

For all of the possibilities that biometric identification technology poses, the truth is that many of these tools are error-prone and cannot reliably identify large swaths of New Yorkers.[3] In particular, facial recognition technology, which attempts to identify a person based on certain facial characteristics, is currently the focus of nationwide concern.[4] This is because facial recognition threatens to place people at unprecedented levels of surveillance as they move about their daily lives, but studies repeatedly find that the technology cannot reliably identify faces that are not white and male.[5] In particular, facial recognition software has been shown to have large error rates in identifying women, people of color, children, the elderly, and people with disabilities.[6]

In response to these concerns, several cities, including San Francisco, Oakland, and Somerville, have banned facial recognition by city agencies.[7] Other state-wide initiatives proposing partial bans or moratoriums are actively moving forward, including in New York and Michigan.[8] Within this regulatory environment, it is disappointing that the legislation proposed by the City Council does not address the unique concerns raised by the deployment of facial recognition by city agencies such as the NYPD.

It is especially concerning because there is a high risk of abuse. Biometric identification technologies make it possible to covertly monitor multitudes of people in public and private spaces at a low cost. This poses serious implications for our basic liberties, including the right to be free from unreasonable search and seizure, as well as freedom of speech, association, and expression.

---

[1] *Community Control Over Police Surveillance: Technology 101*, AMERICAN CIVIL LIBERTIES UNION, www.aclu.org/report/community-control-over-police-surveillance-technology-101.

[2] *Id.*

[3] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROCEEDINGS OF MACHINE LEARNING RESEARCH 1(2018), *available at* http://gendershades.org/overview.html; *see also* Salem Hamed Abdurrahim, *Review On The Effects Of Age, Gender, And Race Demographics On Automatic Face Recognition*, 34 THE VISUAL COMPUTER 1617 (2018), *available at* https://doi.org/10.1007/s00371-017-1428-z; Jacob Snow, *Amazon's Face Recognition False Matched 28 Members of Congress with Mugshots*, AMERICAN CIVIL LIBERTIES UNION (July 26, 2018), www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

[4] *See* Coalition Letter to Elijah Cummings, Chairman, & Jim Jordan, Ranking Member, of the U.S. House Oversight and Reform Committee (June 3, 2019), *available at* https://tinyurl.com/y673fsbv (urging a federal moratorium on face recognition for law enforcement and immigration enforcement purposes); Nicole Martin, *The Major Concerns Around Facial Recognition Technology*, FORBES (Sept. 25, 2019), www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology/#2f3d39534fe3.

[5] Steve Lohr, *Facial Recognition Is Accurate, if You're a White Guy*, N.Y. TIMES (Feb. 2018), https://nyti.ms/2BNurVq.

[6] Buolamwini, *supra* Note 3.

[7] Rachel Metz, *Beyond San Francisco, More Cities Are Saying No To Facial Recognition*, CNN (July 17, 2019), www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html.

[8] Elizabeth Kim, *Albany Lawmakers Introduce Bill Banning Landlords From Using Facial Recognition Technology*, THE GOTHAMIST (May 15, 2019), https://gothamist.com/news/albany-lawmakers-introduce-bill-banning-landlords-from-using-facial-recognition-technology; Steve Neavling, *House Bill Would Ban Facial Recognition Technology In Michigan*, METRO TIMES (July 11, 2019), www.metrotimes.com/news-hits/archives/2019/07/11/house-bill-would-ban-facial-recognition-technology-in-michigan.

Moreover, biometric identification technology is frequently being utilized in low income communities and communities of color, which are already subject to over surveillance.[9]

The NYPD is one of the largest and most technologically advanced police forces in the United States.[10] Unfortunately, it is not one of the most transparent. The NYPD has historically revealed details about its surveillance technologies only after costly Freedom of Information Law (FOIL) litigation, investigative reporting, or being court ordered.[11] This erodes public trust and can lead to abuses of constitutional rights.

For instance, the Brenan Center was party to a multi-year legal dispute with the NYPD to obtain information about the Department's use of predictive policing technologies beginning in June 2016.[12] The NYPD denied our initial FOIL request and subsequent appeal, forcing the Brennan Center to file a lawsuit.[13] In 2017, a judge finally ordered the NYPD to produce records about its testing, development, and use of predictive policing tools.[14] However, it took a full year for the NYPD to comply. Concerningly, the records we eventually obtained indicated that the NYPD had no policy in place to explicitly govern the use of predictive policing, or the sharing and retention of the data produced.[15]

In another example, after extensive FOIL litigation, Georgetown Law's Center on Privacy and Technology obtained records from the NYPD detailing worrying abuse of their facial recognition software. In one striking case, after the technology failed to produce a match for a suspected low-level shop lifter, detectives uploaded an image of similar looking celebrity instead. They sent the resulting matches from a compromised facial recognition analysis to investigating officers, who then used this faulty data to make an arrest.[16]

Similarly, this summer the New York Times reported that the NYPD has been uploading photos of children as young as eleven into its facial-recognition systems.[17] When questioned by reporters, several members of the City Council said they were unaware of the policy.[18] This is because the NYPD does not transparently report on what surveillance technology it is using, its efficacy, or how it stores, analyzes, or shares the information it collects.

---

[9] *Community Control Over Police Surveillance: Technology 101*, *supra* Note 1.
[10] *About NYPD*, NYC.gov, www1.nyc.gov/site/nypd/about/about-nypd/about-nypd (last accessed Oct. 3, 2019).
[11] Dustin Volz, *Privacy Group Sues NYPD For Release Of Facial-Recognition Documents*, REUTERS (May 2, 2017), www.reuters.com/article/us-usa-cyber-face-recognition-idUSKBN17Y1Z1.
[12] Rachel Levinson-Waldman & Erica Posey, *Court: Public Deserves to Know How NYPD Uses Predictive Policing Software*, THE BRENNAN CENTER FOR JUSTICE (Jan. 28, 2018), https://www.brennancenter.org/our-work/analysis-opinion/court-public-deserves-know-how-nypd-uses-predictive-policing-software.
[13] Rachel Levinson-Waldman & Erica Posey, *Predictive Policing Goes to Court*, THE BRENNAN CENTER FOR JUSTICE (Sept. 5, 2017), http://www.brennancenter.org/blog/predictive-policing-goes-court.
[14] *Supra*, Note 13.
[15] *Supra*, Note 12.
[16] *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEORGETOWN LAW'S CENTER ON PRIVACY AND TECHNOLOGY (May 16, 2019), https://www.flawedfacedata.com.
[17] Joseph Goldstein & Ali Watkins, *She Was Arrested At 14. Then Her Photo Went To A Facial Recognition Database*, N.Y. TIMES (Aug. 1, 2019), https://nyti.ms/2GEzuZ8.
[18] *Id.*

A strong local democracy like New York City requires at least a basic level of information about what its local police are doing and how they are doing it, particularly given New York City's history of discriminatory stop-and-frisk policies[19] and because reports show NYPD policing continues to target communities of color.[20]

The Public Oversight of Surveillance Technology (POST) Act, introduced by Council Member Vanessa Gibson, would require the NYPD to disclose basic information about the surveillance tools it uses and the existing safeguards to protect the privacy and civil liberties of New Yorkers.[21] The bill is supported by over half the City Council, with twenty-eight co-sponsors and endorsements from the Black, Latino/a, and Asian Caucus and the Progressive Caucus.

The POST Act is carefully drafted to ensure that the NYPD can continue to keep the city safe, while providing policymakers with the information necessary for effective oversight.[22] It requires the NYPD to issue privacy impact reports, like the reports already published by many federal agencies including Department of Homeland Security (DHS) and the Federal Bureau of Investigations (FBI).[23]

Several municipalities, including San Francisco, Oakland, Berkley, and Seattle have passed more stringent bills, including legislation that bars law enforcement from utilizing new surveillance technologies without City Council approval.[24]

Transparency and oversight are essential features of a strong democracy, and the Brennan Center commends the Council for addressing these critical and timely issues. However, is vital that any legislation requiring transparency on biometric identification technologies also applies to law enforcement.

Thank you again for the opportunity to testify today. I am happy to answer any questions.

---

[19] *See, e.g., Floyd v. City of New York*, 959 F. Supp. 2d 540 (S.D.N.Y. 2013).

[20] *See, e.g., Stop-and-Frisk in the de Blasio Era*, NEW YORK CIVIL LIBERTIES UNION (Mar. 2019), www.nyclu.org/en/stop-and-frisk-data (finding Black and Latino people were more likely to be frisked and, among those frisked, were less likely to be found with a weapon).

[21] New York City Council Int. 0487-2018, *available at* https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0.

[22] For more on Public Oversight of Surveillance Technology Act see "The Public Oversight of Surveillance Technology (POST) Act: A Resource Page, available at www.brennancenter.org/analysis/public-oversight-surveillance-technology-post-act-resource-page.

[23] *Department of Justice/FBI Privacy Impact Assessments*, U.S. FEDERAL BUREAU OF INVESTIGATIONS, *available at* https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments; *Privacy Impact Assessments*, U.S. DEPARTMENT OF HOMELAND SECURITY, *available at* https://www.dhs.gov/privacy-impact-assessments.

[24] The Editorial Board, *San Francisco Banned Facial Recognition. New York Isn't Even Close.*, N.Y. TIMES (May 18, 2019), https://nyti.ms/2LTq80Q.

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 Recognition 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 misused 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_nAlGf9XRl-Unik8xWOh_.

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/.

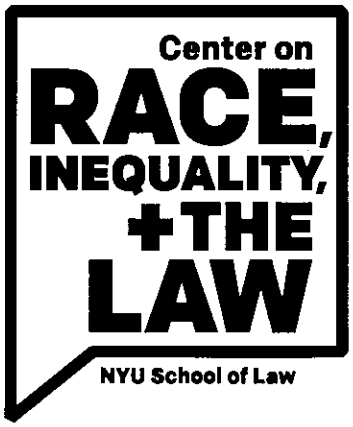
70 *See* "NYPD Installs 'Sky Watch' in Harlem Neighborhood," CrownHeights.info, November 23, 2006, available at: http://crownheights.info/crime/3780/nypd-installs-sky-watch-in-harlem-neighborhood/.

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/.



Testimony of the Center on Race, Inequality, and the Law at NYU School of Law submitted to the Committee on Housing and Buildings, the Committee on Technology, and the Committee on Consumer Affairs and Business Licensing Regarding Oversight of Facial Recognition Technology and Biometric Data Collection in Businesses and in Residences

October 7, 2019

Submitted by:
Vincent M. Southerland
Executive Director
Center on Race, Inequality, and the Law
Adjunct Professor of Law
New York University School of Law
139 MacDougal Street, 416
New York, NY 10012
Telephone: (212) 998-6882
vincent.southerland@nyu.edu

The Center on Race, Inequality and the Law at NYU School of Law presents the following testimony regarding the proposed bills attempting to curb the harmful consequences of facial recognition and biometric data collection technologies in New York City residences and businesses.[1] In the course of our work, the Center has frequently provided commentary and guidance regarding specific technologies, with a focus on the racial justice implications of those technologies across a number of domains. Our comments give voice to the concerns raised by these technologies—specifically their ability to either perpetuate or mitigate racism and inequality in our society.[2] As always, they are also informed by the lives and experiences of people and communities of color who are often disproportionately subjected to the harmful use technological tools.

A Ban on Facial Recognition Technology in Residential Spaces is Warranted

Based on our extensive work in this area, we conclude that there must be an outright ban on facial recognition technologies in New York City residential spaces. The proposed legislation that is the subject of this hearing constitutes a harm reductionist approach that—while well intentioned—falls short of what is required of the city's government to protect all New Yorkers and keep all New Yorkers safe. The only way for our city to ensure that facial recognition technology is not wielded to perpetuate racial inequality and racially-motivated surveillance of New Yorkers is to

---

[1] Given our expertise, the Center's testimony is focused on the use of facial recognition technology in residential buildings and the biometric data that flows from the use of that technology.

[2] For example, the Center, in partnership with advocates and organizations focused on the social justice impact of technology, has offered comments and testimony to the Pennsylvania Sentencing Commission (considering the use of algorithmic risk assessments at sentencing), the Judicial Council of California (considering the use of algorithmic risk assessment in pretrial decision-making), the Illinois Supreme Court Commission on Pretrial Practices (same), and the Missouri Supreme Court (same). Center on Race, Inequality & the Law and AI Now Institute, Statement of the AI Now Institute and NYU Law's Center on Race, Inequality, and the Law on the Pennsylvania Commission on Sentencing's Revisions to the Proposed Sentence Risk Assessment Instrument (Nov. 30, 2018), http://www.law.nyu.edu/sites/default/files/AI%20Now--CRIL%20November%202018%20PA%20Risk%20Assessment--Sentencing%20Commission%20Comments.pdf; Chelsea Barabas et. al, Technical Flaws of Pretrial Risk Assessments Raise Grave Concerns (July 17, 2019), https://dam-prod.media.mit.edu/x/2019/07/17/California.pdf; Chelsea Barabas et. al, Technical Flaws of Pretrial Risk Assessments Raise Grave Concerns (June 30, 2019), https://endmoneybond.org/wp-content/uploads/2019/07/technical-flaws-of-pretrial-risk-assessments-raise-grave-concerns-illinois-supreme-court-submission.pdf; Chelsea Barabas et. al, Technical Flaws of Pretrial Risk Assessments Raise Grave Concerns (July 17, 2019), https://dam-prod.media.mit.edu/x/2019/07/17/Missouri.pdf. The Center was also a principal drafter of, and signatory to, The Use of Pretrial "Risk Assessment" Instruments: A Shared Statement of Civil Rights Concerns, which was endorsed by more than 100 civil rights and racial justice organizations nationwide. The Use of Pretrial "Risk Assessment" Instruments: A Shared Statement of Civil Rights Concerns (July 30, 2018), http://civilrightsdocs.info/pdf/criminal-justice/Pretrial-Risk-Assessment-Full.pdf. The Center's Executive Director is also a member of the New York City Automated Decision Systems Task Force. NYC AUTOMATED DECISION SYSTEMS TASK FORCE, https://www1.nyc.gov/site/adstaskforce/members/members.page (last visited Oct. 3, 2019).

ban it. As we set forth below, legislation has been introduced at the state and federal level to do just that.[3]

We appreciate the vast possibilities that technological innovation holds for improving human life in our society. But with those promises come perils that require bold safeguards.[4] Technology itself does not inevitably foster progress. It is simply a tool that can be wielded for many different purposes, including harmful ends. The hands in which those tools are held often determines how those harms are felt and who bears the disproportionate burden of them. As a result, stakeholders must always fully evaluate the potential impact of any new technology before it is developed and deployed, and its intended and unintended consequences, rather than simply accepting its purported promises at face value.

Experience tells us that the consequences of facial recognition technology clearly outweigh its benefits. That experience is informed by an understanding that Black, Latinx, poor, and working class New Yorkers will unequally bear all of the most extreme burdens if New York City continues to permit the use of facial recognition technologies in the manner contemplated by the proposed legislation. These technologies are being touted as a means to improve public safety, without any evidence whatsoever that they actually do so. At the same time, facial recognition technologies lead to increased surveillance, especially in Black and Brown communities that are already disproportionately and unjustly over-surveilled by law enforcement. Beyond the fact of increased law enforcement surveillance, the potential—and in many ways inevitable—misuse of surveillance data raises additional concerns. There are already many well-documented horrors associated with facial recognition technology across the world from the United States to China[5], including the NYPD's documented abuse of facial recognition technology against children over the last four years.[6] Once biometric data is collected and stored, there are few checks on anyone's use of it or access to it. The collection of biometric data also raises extreme privacy and civil liberties issues. Facial recognition technologies even implicate the Constitutional protections, as these technologies automatically create a chilling effect, limiting free speech and peaceful assembly.[7]

---

[3] State Assembly Bill A7790, introduced by Assemblywoman Latrice Walker in May 2019 seeks to ban the use of facial recognition technology by landlords, while H.R. 4008, introduced by Congresswomen Yvette Clark, Ayanna Pressley, and Rashida Talib would ban the use of facial recognition technology in public housing. No Biometric Barriers to Housing Act of 2019, H.R. 4008, 116th Cong. (2019)

[4] Rashida Richardson, Jason M. Schultz, & Vincent M. Southerland, Litigating Algorithms 2019 US Report: New Challenges to Government Use of Algorithmic Decision Systems (AI Now Institute, September 2019). https://ainowinstitute.org/litigatingalgorithms-2019-us.html.

[5] Claire Garvie and, *America Under Watch: Face Surveillance in the United States,* GEORGETOWN LAW CENTER ON PRIVACY & TECHNOLOGY (May 16, 2019), https://www.americaunderwatch.com/

[6] Joseph Goldstein & Ali Watkins, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database,* N.Y. TIMES (Aug. 1, 2019) https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html

[7] Claire Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Lineup: Unregulated Police Facial Recognition in America,* GEORGETOWN LAW CENTER ON PRIVACY & TECHNOLOGY (October 18, 2016), https://www.perpetuallineup.org/

Facial recognition technologies also have racial discrimination baked into the algorithms and data sets that drive their operation.[8] The pervasive nature of racism and gender bias means that the raw materials used to build these tools, and the technologists and corporations who build them, simply do not fully account for race and gender.[9] Accordingly, it is well established that these tools do not work as accurately on what the system reads as "Black" and "Brown" faces, and also do not work as accurately on what the system reads as "female" faces,[10] assuming that their shortcomings allow them to read these faces at all. These fundamental deficiencies can lead to harmful misidentifications that burden residents of color, their families, friends, and guests. In the residential context, the introduction of this technology would create a two-tiered race-based system, in which white people encounter few hurdles to accessing their buildings using facial recognition technologies, while Black or Brown people are left to grapple with the race-based flaws endemic to the technology. We do not raise this concern to encourage improvements to the design of these technologies, but rather to highlight another way in which facial recognition technologies foster racial inequality, and why New York City should ban them.[11]

Beyond broadening the scope of surveillance and fostering harm because of its flaws, this technology adds to the already striking power differential between landlords and tenants. The coercive effect of a landlord's control over a tenant's biometric data is readily apparent. It can be easily misused for any number of purposes, including to foster evictions. Moreover, there is no way to ensure that landlords limit the use of this technology to entry points in residential buildings; it can just as easily be installed in the hallways and elevators that residents use to access their homes, furthering surveillance and the potential for abuse.

Unfortunately, the proposed protections in the legislation offer little relief. Primarily, these bills deal with issues of notice and consent. But letting Black and Brown New Yorkers, including those who are economically disadvantaged, know that their residences or the places of business that they frequent are using facial recognition technologies and collecting their biometric data does not mitigate the negative impacts of those technologies. In operation, these bills will have the effect of coercing people to consent. And while having a physical key to one's residence is an important protection, it does nothing to stem surveillance and the collection of tenants' biometric data, and does not prevent the invasion of privacy caused by these tools.[12] At bottom, the reforms these proposed bills offer would still allow people to be surveilled in order to literally enter their own homes.

The way forward here is clear. As with all new advances, it is simply not acceptable to sacrifice civil liberties for the convenience of what purports to be

---

[8] Claire Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data,* GEORGETOWN LAW CENTER ON PRIVACY & TECHNOLOGY (May 16, 2019), https://www.flawedfacedata.com/

[9] Joy Buolamwini, *How I'm Fighting Bias in Algorithms*, TEDXBEACONSTREET (Nov. 2016), https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms; Sarah Myers West, Meredith Whittaker, & Kate Crawford, Discriminating Systems: Gender, Race, and Power in AI (AI Now Institute, April 2019). https://ainowinstitute.org/discriminatingsystems.pdf

[10] Garvie, *supra* note 8.

[11] *Id.*

[12] Moreover, practically speaking, residents should have access to their residences with a mechanical key in any event.

technological progress. The potential harms caused by increased surveillance, faulty technology, and the potential for misuse against communities of color outweigh any benefit—if there is any benefit at all—that this technology offers. An outright ban on its use is appropriate.

The Proposed Local Laws Are Insufficient

Our recommendation for a ban is made within the context of our concerns about the shortcomings in the proposed legislation. For example, while each community requires individual consideration, there are jurisdictions that have already led the way in addressing how to balance civil liberties and technology. For example, in 2008, Illinois passed the "Illinois Biometric Information Privacy Act" (BIPA), which includes some of the strongest protections in the country against biometric privacy violations. For example, BIPA requires:

- Public agencies and private entities to obtain consent from a person before collecting or disclosing their biometric information
- When the purpose of collection ends, that the agency destroys such identifiers in a timely manner, and in no event more than three years after the last contact with the subject
- The secure collection of such identifiers, under standards regulated by statute
- The ready availability of civil action by individuals against such agencies that violate the rules.[13]

This law (and others like it that have subsequently been signed into law in states like Washington and Texas[14]) makes significant strides in ensuring that people have control over how their most personal and sensitive information is used. Proposed Local Law Int. 1672-2019, and its requirement that businesses submit registration statements regarding technology used on the premises, while well-intentioned, includes few of the same protections. The proposed legislation is silent regarding: the storage and security of the data collected; limits on who landlords can share information generated by the technology; independent validation of the technology; the need to secure the informed consent of those who might be subjected to the technology; and the need for transparency regarding landlords' economic incentives to install such technology. Without additional provisions to address these concerns, a registration requirement names the problem without actually addressing it.

Proposed Local Law T2019-4579's requirement that residents be provided a mechanical key to access their residence, as a means to allow those residents to opt out of keyless, facial recognition technology entry systems, while well-intended is likewise insufficient. At a bare minimum, where the technology is used there should be meaningful alternatives for residents who wish to opt out of a system that makes their continued residence contingent upon the surrender of personal and potentially

---

[13] 740 ILCS 14/ Biometric Information Privacy Act (2008).

[14] Molly McGinley, Kenn Brotman & Erinn Rigney, *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States,* THE NATIONAL LAW REVIEW (March 25, 2019) https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states.

incriminating[15] biometric information. The inherent power imbalance between tenants and landlords suggests that any real agency might be minimal. Low-income tenants in particular, when forced to choose between asserting their right to a mechanical key or, in the alternative, assenting to their biometric acquisition, will too often choose the latter when their ability to sign a lease appears contingent upon their consent to being surveilled and scanned. Provisions that addresses this concern, including penalties to be imposed against landlords who discriminate or retaliate against residents who decline to be subjected to this technology should be added to the proposal.

Notwithstanding the issues we have raised regarding the proposals, we recommend that any decisions that allow the use of this technology be made with the feedback, guidance, and input of communities who will be effected by it. If this technology is meant to serve New Yorkers, those same people should be able to decide when and how their own biometric data is going to be collected and used. The failure to provide communities with an avenue for ongoing, rigorous, oversight and accountability would be unacceptable.

Conclusion

The best solution to address the concerns raised by biometric and facial recognition technology in residential spaces is to ban it. While New York City is considering enacting regulatory reforms, other cities have banned the technology's use altogether, while federal legislation is under consideration to do the same. This year, the San Francisco Board of Supervisors voted 8-1 to prohibit all police and city agencies from using facial recognition technology except where they receive special permission of the Board. Oakland, California and Somerville, Massachusetts may soon follow suit. Ten members of Congress introduced H.R. 4008 this year, which would ban the use of biometric technology in all federally funded public housing,[16]and New York State legislators have proposed a similar ban.[17] New York City should take stock of these trends and take action in accordance with them.

Ultimately, facial recognition technology is being used to determine who and who does not "belong." The racial bias that is baked into these technologies is, itself, a signal to New Yorkers about who does and does not "belong." As the abuses outlined at the outset of this submission make clear, this technology has already been deployed by those who have used it to marginalize and oppress communities of color and vulnerable populations. We know that the negative impacts of facial recognition and technologies like it far outweigh any purported benefits. Understanding that reality, New York City should take steps to ban its use in residential spaces.

---

[15] Garvie, *supra* note 5.

[16] Madeline Gregory, *Congresswomen to Propose Ban on Facial Recognition in Public Housing,* VICE NEWS (July 23, 2019), https://www.vice.com/en_us/article/mb889q/congresswomen-to-propose-ban-on-facial-recognition-in-public-housing.

[17]Amy Plitt, *New York lawmakers seek to ban facial recognition technology in rental buildings,* CURBED *(May 7, 2019)* ://ny.curbed.com/2019/5/17/18629120/nyc-buildings-facial-recognition-technology-ban.

10/7/19

FOR THE RECORD

Good Morning City Council Members,

My name is Isabel Reyna Torres. I have lived in Knickerbocker Village since 1997. Knickerbocker Village is a gated community and since that time we were using key cards to enter the complex and the 12 buildings in Knickerbocker Village. After Hurricane Sandy, Knickerbocker put up a facial recognition system. Residents received a letter stating that we needed to have pictures of our faces and this was the only way we can enter the complex and enter our buildings. Many tenants were concerned about scanning our faces. I was one of those tenants that had many concerns about facial recognition being used in KV. Management and owners didn't let tenants know that this was happening, furthermore they never asked for our permission to be able to use this kind of technology in our development. This technology cost over $500,000 to install.

As a tenant leader at KV, in 2014 the Knickerbocker Village Tenant Association made this clear at a public hearing at PS 1 during one of the first massive rent increases. WE never asked for it and WE shouldn't have to pay for technology that infringes on our rights. After Hurricane Sandy, Knickerbocker had many concerns at KV. Security at KV was never one of those concerns. After Hurricane Sandy hit our area, we were left with no heat or electricity. For the two weeks we were without electricity, the facial recognition system didn't work. We weren't only left without essential services, but also without security. Since the doors had to stay open for anyone to enter.

I hope that City Council takes a position that cameras in residential buildings are against a community's rights to live without landlords infringing on those rights. I've always known that what happened in our development was simply wrong and I thank the City Council for putting this bill forth. I hope tenants' voices are heard today.

Thank You,

Isabel Reyna Torres

Attachments included

Assemblyman
SHELDON SILVER
64th District

THE ASSEMBLY
STATE OF NEW YORK
ALBANY

FOR THE RECORD

250 Broadway
Suite 2307
New York, New York 10007
(212) 312-1420
FAX (212) 312-1425

November 16, 2012

Ms. Isabel Reyna
36 Monroe St Apt Db6
New York NY 10002-7724

Dear Ms. Reyna,

It has been far too long a wait, but by now you should have electricity and heat in your apartment. I understand that the amount of time it took for essential services to be restored at Knickerbocker is unacceptable. You have been forced to endure treacherous conditions, and I will continue to work as hard as possible to ensure that, should such an emergency happen again, the response from ownership and management will be far better.

Recently, I hosted a meeting, along with other local elected officials, for Knickerbocker residents to ask questions of your building owner, Con Edison and the Federal Emergency Management Agency (FEMA). Before the meeting, I asked Knickerbocker's owner, AREA Properties, to give tenants a credit on their rent for time spent without essential services (power, heat or hot water).

You and your neighbors have suffered greatly in the aftermath of Hurricane Sandy and I believe, at the very least, you should be given financial relief. I am pleased to say that at the meeting, AREA Properties announced that it will in fact not charge tenants for those days. It is my understanding that those of you who spent the days without power and electricity at a hotel or renting another apartment may be eligible for financial assistance from FEMA. Please visit www.fema.gov/sandy or call (800) 621-3362 to learn more.

I also received a commitment that management will inspect water-damaged apartments, which they had not yet done. To improve communications between management and tenants, I asked that a phone line be set up that you can call for information. That phone number is (646) 287-6676. Please visit the management office or call that number if you are still having problems with power or heat.

If there is anything further I can help you with, please do not hesitate to contact my office at (212) 312-1420 or silver@assembly.state.ny.us.

Sincerely,

SHELDON SILVER
Member of Assembly

SS:je

FOR THE RECORD

April 11, 2013

James Simmons
Area Property Partners
60 Columbus Circle, 20th Floor
New York, NY 10023

Dear Mr. Simmons:

In the aftermath of Superstorm Sandy, we all worked hard together to help residents of Knickerbocker Village recover. As we continue that effort, we are hoping to resolve one of the outstanding problems that remain: The unpaid rent credits that Area Property Partners promised to Knickerbocker tenants for the days they were without essential services following the storm.

At a meeting convened for tenants in November, in which we all participated, you publicly stated that residents would not have to pay rent for the days they were without services. Further, a commitment was made that the money used to refund rent payments would not in any way be at the expense of the tenants. We expect you to fulfill that commitment.

It has now been more than five months since Sandy hit and we are asking that you provide Knickerbocker tenants with the financial relief they were promised. As you know, Knickerbocker residents suffered enormously after the storm, enduring days and weeks in cold and darkness, without heat, light, or elevators.

We understand that the impact of the storm was enormous and the recovery has been long and difficult. However, we expect that your commitment to issue rent credits will be honored. We therefore request you advise us and the tenants in writing as to why they have not received a rebate and when they should expect to receive it. Thank you.

Sincerely,

Senator Daniel Squadron

Assemblyman Sheldon Silver

Borough President Scott Stringer

Council Member Margaret S. Chin

Testimony of FITZROY A. CHRISTIAN

FOR THE RECORD

FOR THE RECORD

JOINT HEARING OF THE NEW YORK CITY COUNCIL COMMITTEE ON HOUSING AND BUILDINGS; COMMITTEE ON TECHNOLOGY; AND COMMITTEE ON CONSUMER AFFAIRS AND BUSINESS LICENSING

ON

FACIAL RECOGNITION ENTRY SYSTEM TECHNOLOGY IN RESIDENTIAL PROPERTIES

City Hall
Monday, 7th October, 2019

Honorable Members of the City Council,

My name is Fitzroy Christian. I reside in the Highbridge community of southwest Bronx, and have been a tenant in my rent stabilized apartment since 1976. I have experienced the Bronx suffering through the "fires", State and municipal disinvestment, planned shrinkages, and outright "benign neglect". For decades, I have been a part of my community's struggles to rebuild our beloved borough, and to restore, maintain, and expand truly affordable housing for the residents, whose resilience, "sweat equity", and determination have constructed the foundation on which today's Bronx is being rebuilt. I have been a member of several community-based organizations and a participant in many local, city- and state-wide coalitions fighting for, among other causes: affordable housing, tenants' rights, reforming the Housing Court system, the Right to Council, Rent Justice, reforming the state's housing laws, and building viable communities where current Bronx resident can stay and newcomers join in expanding the borough's already integrated social, cultural, economic, and ethnic diversity. I have also been involved in campaigns to reduce the over- surveillance and over-policing of our communities, which have had a devastating racial impact on the residents, the vast majority of whom are Black, Brown, and poor.

Thus, it is with great dismay that I witness the unregulated installation and use of facial recognition entry systems and other biometric technologies into apartment buildings located almost exclusively in communities primarily of Black, Brown, and poor people. This is an addition of yet another layer of surveillance on an already over-surveilled racial and ethnic demographic. It provides unfettered and unconstrained opportunities for additional landlord harassment of very vulnerable members of our communities who lack the resources to resist this new assault on their ability to realize the peaceful, quiet, safe, secure, and healthy enjoyment of their homes.

This is a threat to a targeted section of our city's population who have been battered by racial, class, and ethnic warfare for almost the entire existence of this nation, and must not be allowed to continue.

This testimony is a call for the New York City Council to ban or impose a five-year (at the very least) moratorium on the installation and use of any and all forms of biometric technology in residential apartments in New York City until at such time that the Council has conducted a thorough, exhaustive

study and analysis of the technology and has put into place the necessary adequate and comprehensive protections and regulations governing use of such technologies in apartment buildings. It also is a call for the Council to order the de-activation of all currently in-use biometric entry systems and the restoration of the previous mechanical and/or electronic key or key fob systems. Additionally, I am entreating the Council to enact legislation barring the Council from any and all actions or undertakings in relation to the introduction of legislation regarding, or the licensing, permitting, installation, and deployment of biometric and/or other facial recognition entry system technologies in residential spaces in New York City. Furthermore, the sponsors of these two bills being commented upon today, Council Members Brad Lander and Donovan Richards, are called upon to withdraw Intro T4579 and Intro T1672, which they have respectively sponsored, until the aforementioned regulations and protections have been put in place.

Virtually all studies and analyses conducted on the efficacy of biometric/facial recognition technologies have produced consistently dire warnings and examples of the inherent biases, inaccuracies, and unfavorable consequences on people of color, both actual and potential, of the deployment of this technology. A well noted example of this is the American Civil Liberties Union's study and test of one of the leading facial recognition technology systems currently in use by police forces, in which 28 members of the U.S. Congress were falsely matched with mugshots of people who have been arrested or convicted of crimes. [(1)]

As the ACLU stated in its report, *"... the false matches were disproportionately of people of color, including six members of the Congressional Black Caucus, among them civil rights legend Rep. John Lewis (D-Ga.). These results demonstrate why ... the ACLU [is] calling for a moratorium on ... use of face surveillance."*

There are voluminous amounts of research data, studies, reports, symposia, conferences, and articles that universally call for a much more comprehensive development and refinement of the technology, and the absolute need for governments legislating and enforcing thorough across-the-board protections and regulations before these technologies are deployed in residential spaces.

Without protections and regulations, widespread use of the technology would result in a disaster of humongous proportions. The technology is fraught with racial and gender biases [(2)], is untested and unproven, and has met with almost universal condemnation in academia, the tech universe, the general population of nations around the world, and even a number of states and municipalities in this country.

Yet in the face of the massive amount of data supporting a ban or at least a suspension of the use of the technology, these two pieces of legislation are conspicuously silent on the major objections voiced universally:

the collection, use, storage, security, retention, sharing, access to, sale, biometric data ownership, tenant options, accuracy, debiasing, and transfer of tenants' biometric data.

The United States condemns China for its use of the technology as a tool to surveil portions of its population. Here, in the United States of America, several states and cities have enacted legislation to regulate the technology and, in some instances, have passed legislation banning its use until regulations have been put in place.

The bills introduced by Council Members Lander and Richards implicitly accept and condone the installation of the technology. They come with meaningless provisions for use of the technology to be registered with a city agency and for landlords to inform tenants of the technology's use and be given the option to not participate.

I am calling on the City Council to immediately halt all efforts to provide cover for the installation and use of the technology in residential buildings until comprehensive empirical studies are made, and regulatory structures and processes put in place at the federal, state, and municipal levels of government, with rigid oversight.

The social and economic costs to the country and to the hosts of communities of color within these borders would be detrimental and incalculable. But it is avoidable.

Thank you for allowing me to provide this brief overview of my opposition to the use of this technology in residential spaces. I am also including the links below so you can read the full studies and data notated above.

(1) https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

(2) http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

October 7, 2019

Dear Committee members,

My name is Christina Zhang and I am one of the co-chairs of the Knickerbocker Village Tenant Association (KVTA) representing 1,589 families. Knickerbocker Village is an affordable housing complex located in the Two Bridges neighborhood.

Around 2013-2014, Knickerbocker Village installed a facial recognition system in each of the twelve building lobbies in the complex as well as two of the gate entrances into each courtyard. This was done without the consent of tenants, and management has never applied to HCR for permission to install the cameras. KV owners then sought a 14.5% rent increase in 2014 shortly after the installation of the cameras.

Many tenants have complained at KVTA meetings that the technology frequently does not work. They have trouble entering their buildings and must wait for people leaving or entering to go through the doors. The cameras located at the rear gates to the courtyards are especially problematic as sunlight hitting the lenses prevents them from functioning properly. Guards usually end up buzzing people in. Other tenants have mentioned cameras not working late at night, and if the security guards are not there, they are stuck waiting outside or must walk around the block to the front gates. At one point, the former manager mentioned to KVTA building representatives at a meeting that contractors for the camera system were making weekly visits to fix or update the cameras (and at what cost?).

There are many news articles that mention how facial recognition technology is biased against women and people of color. The population at Knickerbocker Village is about 70% Asian. The camera matched the face of one of my cousins to a tenant, and she was able to enter my building, but she does not live here.

I am also personally worried about how the data is being used and stored. Is management sharing this data with government agencies like the NYPD or ICE? How securely is this information being stored? What controls are in place to protect privacy?

Management insists that the cameras were installed for safety, but how does the technology provide this when people can just follow others inside and security guards will buzz in anyone who looks like they're having trouble with the cameras? How necessary is this expensive system for people just looking to return home?

Thank you,

Christina Zhang
32 Monroe Street BA9
New York, NY 10002

October 7, 2019

Committee on Housing and Buildings
Committee on Technology
Committee on Consumer Affairs and Business Licensing

Josh Steinbauer
joshsteinbauer@gmail.com

RE: Key FOB Hearing -- Tenant Statement

From 2006 to 2014, I lived in a loft building in South Williamsburg. It was a community of creative folks in numerous units of live/work spaces. In 2014, the building was served with a Vacate order and all of us were locked out of our homes without access to our possessions despite being protected tenants with provisional loft law coverage. Numerous legal actions were required and the residents were sunk into over a hundred thousand dollars in legals costs. When, after four years, we finally won and regained entry, we found our landlord had brokens and propped windows open. This effectively turned our homes into a pigeon coop, and destroyed all our possessions. We also found that we could not access the building with our old keys and instead the doors were changed to a FOB system. We were each given only one key. Our landlord has refused to provide us with any key fobs for guests, even though that is legally required. There is no backup system (also a legal requirement) so that if the computer crashes we will all be locked out. At one point, when a FOB key was lost, the landlords demanded that we come to their office and pay them $35 for a replacement. What's more dreadful is the incessant tracking and surveillance that FOB keys offer. The residents know from previous and ongoing lawsuits, that our landlord is hostile and litigious. Personally, I know through the course of the legal battle for loft law protection that the landlord's lawyer tried to use my out-of-town work as a means to exclude me from coverage. While my out-of-town work turned out to be completely legal, it forced me to dig up a seemingly endless paper trail of receipts, check stubs, and bank statements in order to prove. Unfortunately, the FOB system is simply the means for the landlord to eventually try it again and bring me to court, not because it will be more true now, but to bury me in legal fees. To me, it feels like ongoing, daily harassment. There's something fundamentally unethical about residents being subjected to tracking and surveillance simply for exercising their tenant rights.

Thank you for your time.
Josh Steinbauer

Legal Services NYC

Testimony of Samar Katnani, Deputy Director
Tenant Rights Coalition (Brooklyn), Legal Services NYC

New York City Council Committee on Housing and Buildings, Committee on Technology, and Committee on Consumer Affairs and Business Licensing

October 7, 2019

My name is Samar Katnani and I am a Deputy Director at the Tenant Rights Coalition at Legal Services NYC. Legal Services NYC (LSNYC) is the largest civil legal services provider in the United States, with deep connections to the communities we serve at our neighborhood-based offices throughout New York City. Our staff members assist more than 110,000 low-income New Yorkers each year. In particular, the Tenant Rights Coalition is at the forefront of the fight to prevent evictions, preserve affordable housing, combat harassment, and ensure that New York City tenants' homes are safe and in good repair. LSNYC welcomes the opportunity to give testimony before the New York City Council's Committee on Housing and Buildings, Committee on Technology, and Committee on Consumer Affairs and Business Licensing.

Facial recognition technology is expanding rapidly, with little to no formal oversight, throughout the country. The use of this nascent technology raises significant concerns, particularly for already vulnerable and marginalized communities of color.[1] For that reason, cities like San Francisco, Oakland, and Somerville have passed legislation banning the use of facial recognition by the government. Legislation is pending here in our own State Assembly (A7790, Latrice Walker) and Senate (S5687, Brad Holyman) that would ban the use of facial recognition technology in the residential context by landlords, and corollary federal legislation—

[1] Woodrow Hartzog, *Facial Recognition is the Perfect Tool for Oppression*, Medium, Aug. 2, 2018, available at https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 (last visited Oct. 6, 2019).

the No Biometric Barriers to Housing Act—has been proposed to ban the use of the technology in public housing. These bills were introduced in response to the total absence of any regulation around the use of facial recognition technology by landlords, particularly where the technology is being introduced in more and more residential buildings. We know of at least four residential buildings across New York City where facial recognition technology has already been installed,[2] and we continue to learn of more on a regular basis.

We would like to address the two proposed pieces of legislation during today's hearing that relate to residential spaces, Intro No. 1672 and the preconsidered Keep Entry to Your Home Surveillance-Free ("KEYS") Act, introduced by Councilmember Richards and Councilmember Lander, respectively. We appreciate that the Council is giving attention to the use of facial recognition technology and recognizing that there is a legislative void that must be filled to protect New York City tenants in this context. Our comments are informed by the efforts and advocacy of a group of Brooklyn tenants we represent, who are fighting against the use of facial recognition technology in their homes, a fight that spurred the above-mentioned State and federal bills.

For the past year, LSNYC's Tenant Rights Coalition been working with over a hundred households that reside in two large buildings in Brownsville, Brooklyn called Atlantic Plaza Towers located at 216 Rockaway Avenue and 249 Thomas S Boyland and owned by Robert Nelson. Over 700 households reside in these two buildings, which were formerly Mitchell Lama buildings and are now rent-stabilized pursuant to a regulatory agreement with the City. The vast majority of the residents of Atlantic Plaza Towers are black and brown women and elderly people. In the fall of 2018, tenants began receiving notices from the New York State Housing &

[2] 1290 Rodman Place, Bronx 10460; 655 Morris Avenue, Bronx 10451; 111-17 Northern Boulevard, Flushing 11369; 10 Monroe Street, New York 10002 (Knickerbocker Village).

Community Renewal that their landlord had filed an application seeking approval from the state agency to install a facial recognition system called StoneLock. The application was three pages long and included no information about the technology.

Alarmed by the prospect of such technology, the tenants immediately began organizing and educating themselves about facial recognition. What they learned was frightening, and they concluded that nothing short of a ban of such technology in residential spaces would adequately protect them and other New York City tenants. In the course of our work with the Atlantic Towers tenants, we, along with the tenants, have not ascertained any compelling justification for the use of facial recognition technology and the collection of biometric data by landlords. Conversely, there are many significant risks and dangers to residential tenants that make these technologies deeply concerning. This was captured in the San Francisco ordinance referenced above: "The propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits, and the technology will exacerbate racial injustice and threaten our ability to live free of continuous [ ] monitoring."[3]

As such, while we welcome the Council's efforts to attend to this emergent issue for residential tenants, we do not believe the two bills do enough to protect New York City tenants given the dangers posed by biometrics collection in the residential context.

When Landlords are Permitted to Collect Biometric Data, Tenants are at Risk of Irreparable Harm

It is universally understood that "biometric data typically refers to any information that is used to identify a natural person based upon unique physiological identifiers (e.g., fingerprint, face, eye, or voice)."[4] Notably, biometric data is further considered to be personal identifying

[3] Stop Secret Spying Ordinance, Section 1(d).

[4] Jonh T. Wolak, Mitchell Boyarsky, and Randy A. Gray, Daniel J. Tucker, Outside Counsel, *The Biometric Standards: How New York Measures Up in the Face of Biometric Use Regulations*, NYLJ, Jun. 4, 2018 at S3, col 1.

information, "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual."[5] Biometric data cannot be simply reissued in the same was as other kinds of individual data—a person's facial image is theirs for life—and therefore the ramifications of having one's biometric data compromised mandates an extremely high threshold of restriction and oversight.

Without any regulation in place to protect tenants before or after a data breach—regulation that is not provided for in Intro No. 1672 and the KEYS Act—tenants are left susceptible to identity theft, which is already a very real and serious threat to a person's ability to succeed in low-income communities of color. Biometric identifiers reveal sensitive information, not only because they are unique characteristics, but because they are permanent. A data breach would expose tenants whose biometric data is stored with their landlord to severe privacy and security threats, and the growing rate of data breaches across commercial industries cast serious doubts on the ability of landlords to protect biometric information collected from tenants.[6] Most distressing is the fact that, unlike a compromised password or stolen credit card and bank information, a person's biometric identifier can never be replaced.[7]

---

[5] U.S. General Services Administration, Rules and Policies - Protecting PII - Privacy Act, https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act; see also An Act relative to consumer data privacy, Bill No. 120, Massachusetts Senate (2019) (states that "personal information" includes pseudonymized information because it "is capable of being associated with [...] a particular consumer.").

[6] See Charles Warzel & Stuart A. Thompson, *Tech Companies Say they Care*, NY Times, Apr. 10, 2019, https://www.nytimes.com/interactive/2019/04/10/opinion/tech-companies-privacy.html; see also Danny Palmer, *The Hacking Strategies that will Dominate 2019*, ZDNet, Feb. 15, 2019, https://www.zdnet.com/article/the-hacking-strategies-that-will-dominate-in-2019/.

[7] See Claire Gartland, *Biometrics are a Grave Threat to Privacy*, NY Times, Jul. 5, 2016, https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-are-a-grave-threat-to-privacy ("[I]nstead of credit monitoring, will breached companies offer their customers plastic surgery?").

All Current Facial Recognition Systems Have Accuracy and Bias Problems

To our knowledge, there is not a single facial recognition system on the market today that is flawless, and all have limitations. Even prevailing facial analysis systems owned and operated by leading technology companies, such as IBM, Microsoft, and a Chinese company called Megvii, makers of Face++, have shown serious discrepancies in accuracy rates based on gender and skin type. By construction, these systems are based on statistical methods which must account for uncertainty. Study after study has proven that these artificial intelligence systems "rely on machine learning algorithms . . . trained with biased data [that] have resulted in algorithmic discrimination."[8] These particular facial recognition systems have been "proven to perform better on lighter-skinned men than darker-skinned individuals and women."[9]

Gender Classifier	Darker Male	Darker Female	Lighter Male	Lighter Female	Largest Gap
[illegible]	94.0%	79.2%	100%	98.3%	20.8%
[illegible]	99.3%	65.5%	99.2%	94.0%	33.8%
IBM	88.0%	65.3%	99.7%	92.9%	34.4%

Figure 1. Intersectional Skin Type and Gender Classification Accuracy Disparities. www.gendershades.org

[8] J. Buolamwini and T. Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Conference on Fairness, Accountability and Transparency, 77–91 (2018), available at https://www.media.mit.edu/publications/gender-shades-intersectional-accuracy-disparities-in-commercial-gender-classification/, (last visited Apr. 30, 2019); see also Matt Wood, *Face recognition researcher fights Amazon over AI bias*, AP News, 2019, available at https://www.apnews.com/24fd8e9bc6bf485c8aff1e46ebde9ec1 (last visited Apr. 30, 2019).

[9] Id.

Following Gender Shades, the leading study on the impact demographic and phenotypic characteristics (i.e., gender and skin type, respectively) have on automated facial analysis accuracy, another study performed for the Science and Technology Directorate of the Department of Homeland Security ("DHS-S&T") demonstrated similar algorithm performance issues using benchmarks accounting for phenotypic characteristics (i.e., physical skin properties that vary amongst different ethnicities).[10] In addition to other demographic factors, the DHS-S&T study used skin reflectance as one of the benchmarks to test facial biometric systems. Skin reflectance is a phenotypic measure that relies on light intensity measurement at specific wavelengths to determine the physical skin properties, instead of capturing color spaces optimized for human perception to determine "skin color."[11] The study discovered that skin reflectance, and not racial category, was a better way to assess for accuracy. The performance of a face recognition system was found to be less efficient or accurate for people with lower (or darker) skin reflectance.[12]

Not only are the benchmarks used to test for diverse demographics and phenotypic attributes extremely important, but so are the conditions in which the facial recognition system is tested. What might function well in a controlled lab-setting is not likely to operate at the same level of efficiency in the day-to-day circumstances of the real-world. Every new technology boasts to be better and more improved than the last, but without independent validation studies proving these claims, there is no guarantee these systems will not discriminate against people of color. Without publicly available information regarding the machine-learning techniques and the

[10] C. M. Cook, J. J. Howard, Y. B. Sirotin, J. L. Tipton and A. R. Vemury, "Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems," IEEE Transactions on Information Forensics and Security, 2019, available at http://jjhoward.org/pubs/demographic-effects-image-acquisition.pdf (last visited Apr. 30, 2019).

[11] Id. at 3.

[12] Id. at 2.

training data used to build the algorithm used by a facial recognition system, which companies are not required to provide, the system cannot be trusted to operate effectively and without bias. Even if accuracy disparities are within a few percentage points, a substantial number of the City's millions of tenants will be affected.

The racial impact of the inadequacy of these systems, many of which we understand have not been used before in the residential context, is likely also why facial recognition technology is being deployed first and foremost in buildings housing primarily people of color. These technologies heavily rely on large-scale biometric data collection for development and evaluation. The face data from the City's tenants of color will be a valuable collection of highly sought after biometric face data. The risk of commercial exploitation of the visible light images and near-infrared face templates that would be collected and stored from the tenants is very plausible given the current lack of face data from people of color and other underrepresented groups in large-scale face datasets. Already technology companies have resorted to extreme measures to collect such information. A Chinese company, named CloudWalk, has reportedly arranged a deal with the government of Zimbabwe to provide face surveillance technology access to the valuable biometric data of the country's citizens.[13] Similarly, the New York Daily News recently reported that Google funded a project that undertook dubious tactics to collect face data from people of color, including homeless individuals, in order to build a massively diverse database for its upcoming smartphone that currently suffers from racial bias.[14] Allowing the deployment of facial recognition technology on the City's tenants of color is tantamount to

[13] Amy Hawkins, *Beijing's Big Brother Tech Needs African Faces*, Foreign Policy, Jul. 24, 2018, https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/ (last visited Oct. 4, 2019).

[14] Ginger Adams Otis and Nancy Dillon, *Google using dubious tactics to target people with 'darker skin' in facial recognition project: sources*, New York Daily News, Oct. 2, 2019, https://www.nydailynews.com/news/national/ny-google-darker-skin-tones-facial-recognition-pixel-20191002-5vxpgowknffnvbmy5eg7epsf34-story.html (last visited Oct. 4, 2019).

monetizing their biometric data, not for their benefit, but for the profit of the technology vendors, and quite possibly the landlords who may be compensated for installation of these systems in their buildings. This is extremely troubling.

Risk of Harm to Communities of Color & Potential Abuse by Law Enforcement

Given the overall demographics of the population of New York City renters and what we know about the demographics of the tenants residing at affordable, regulated residential buildings where the technology is already installed or proposed to be installed, allowing landlords to deploy facial recognition technology will only serve to further surveil black and brown tenants, for whom privacy concerns pose a greater threat. Whether the act of surveillance is at the hands of private actors or the state, it "is often the gateway to very tangible harms."[15] In addition to surveillance by law enforcement that too often results in violence, black and brown communities are only further pushed to the margins because surveillance and the feeling of being watched generates a fear and uncertainty that leads people to "self-police" and inhibits activity in public space.[16] As Congresswoman Ayanna Pressley stated in connection with the introduction of No Biometric Barriers to Housing Act, "Vulnerable communities are constantly being policed, profiled, and punished, and facial recognition technology will only make it worse." The San Francisco legislature noted in its ordinance banning the use of facial recognition that "[w]hile surveillance technology may threaten the privacy of all of us, surveillance efforts have historically been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective."

---

[15] Chris Gilliard, *Privacy's not an abstraction*, Fast Company, Mar. 25, 2019, https://www.fastcompany.com/90323529/privacy-is-not-an-abstraction (last visited Apr. 30, 2019).

[16] See id.

Furthermore, there is nothing protecting tenants from landlords or biometrics technology companies sharing their biometric data with governmental agencies such as the NYPD or ICE, with or without a subpoena, or selling it to third-parties. The biometric data collected, used, and stored by a landlord could be requested by law enforcement authorities or third parties who could use it with other facial recognition systems and expose tenants to new risks. It could expose tenants to police profiling, false accusations,[17] or wrongful arrests.[18] Once in the hands of a third-party, the data could be further exploited or jeopardized. Given these tangible risks and the grave consequences, tenants should not be forced to share their biometric data and live with fear of it being shared with law enforcement, in order to rent an apartment in New York City. Given the challenges people of color experience when trying to secure housing in a rapidly gentrifying and discriminatory housing market, both the coercive effect and the adverse consequences of biometrics will disparately impact tenants of color.

Even if Tenants Have a Statutory Right to Refuse Biometrics Collection, the Majority of Tenants Do Not Have the Power to Exercise That Right

In our experience, tenants are not calling for or seeking the installation of this technology in their homes. Landlords are unilaterally making these decisions, exerting control over tenants and their biometric data based on property ownership and the inability of tenants to easily find alternative housing. The only purported purpose for installing facial recognition technology provided by landlords to date is to "improve" security. However, tenants do not feel unsafe, and do not believe that facial recognition technology will do anything to make them safer. In fact,

---

[17] Jeremy C. Fox, *Brown University student mistakenly identified as Sri Lanka bombing suspect*, Boston Globe, Apr. 28, 2019, https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html (last visited Oct. 4, 2019).

[18] Bah v. Apple Inc., 19-cv-03539, U.S. District Court, Southern District of New York, (April 2019)(18-year old African American teenage boy misidentified in Apple Stores sues for $1 Billion in damages), available at https://www.scribd.com/document/407291893/Bah-v-Apple-Inc-19-cv-03539-U-S-DistrictCourt-Southern-District-of-New-York (last visited Oct. 4, 2019).

many of the buildings where facial recognition is already installed or proposed already have robust security systems that include security guards and cameras and key-fob entry systems. For example, Morris Avenue Apartments at 655 Morris Avenue in the Bronx, a new 176-unit building opened for formerly homeless veterans, boasts "[a]n extensive DVR-security camera system with approximately 175 cameras."[19] The same goes for Atlantic Plaza Towers where 360-degree cameras span every inch of the two-building complex except in the stairwells. Tenants believe that a facial recognition entry system will not do anything to meaningfully supplement or enhance security. To the contrary, tenants rightfully worry about increased instability in their affordable housing and increased gentrification of their communities through increased surveillance by their landlord, who may misuse the data collected in eviction cases or install the technology to attract wealthier tenants and collect higher rents.

We appreciate that the "opt out" provision of the KEYS Act seeks to mitigate these harms and imbalance by requiring landlords to offer key alternatives and prohibiting a landlord from "requiring" a tenant use facial recognition technology. We have recently learned that prospective tenants at an affordable housing lottery building in the Bronx—1290 Rodman Place—were required to accept the use of facial recognition technology *and* scan their faces into the system at the time of lease signing. To our knowledge, this was presented to tenants as a requirement, with no opt-out. While under the KEYS Act a landlord should not be able to condition the signing of a lease upon consenting to the use of technology, imagine a person, perhaps living in shelter or facing possible eviction, sitting in a room with a landlord or its agent and being presented a lease for an apartment; or most New York City apartment-seekers who find it incredibly difficult to obtain housing in our increasingly tight and unaffordable rental

[19] https://www.prnewswire.com/news-releases/omni-new-york-llc-celebrates-opening-of-176-units-of-leed-certified-affordable-housing-for-families-and-formerly-homeless-veterans-300409398.html

market. The practical reality is that the prospective tenant almost always acquiesces to whatever conditions or preferences a landlord sets, given that the housing is in control of the landlord and desperately sought by the person. The notion that a prospective tenant can freely give consent to facial recognition technology when signing a new lease does not account for the vulnerable position of tenants seeking housing and the power imbalance between tenants seeking housing and landlords who control access to that essential resource.

Moreover, the bill does not require that the landlord obtain consent of any kind, informed or not. It does not specify what information the landlord must provide or that the landlord must supply a clear statement that the tenant has the right to decline under City law. It does not take into account the wide range of education and literacy levels that make up the City's tenant base or language access issues. The significance of biometric data is not known to most, details regarding data collection, retention, and security are complicated, and issues with accuracy and bias are nuanced and not commonly known. A landlord could simply tell a tenant that there is new "cool," state-of-the-art technology that will allow them to easily enter their homes, or choose any manner of framing the "choice" in a way that makes clear the landlord's preference or obfuscates any issues with the technology. In fact, through our work, we are aware that this actually has been the way some landlords have presented these types of technology to tenants. We believe because of the inherent power imbalance between landlords and tenants, that an opt out alone will not have the impact sought, in terms of giving tenants a meaningful choice to decline the use of the technology, particularly where no informed consent is required. In the absence of creating a meaningful choice for tenants, there is then the risk that this bill will inadvertently sanction landlords' collection of biometric data, creating a situation where New York tenants must turn over their biometric data to a private actor in order to obtain or retain a home.

Furthermore, how these facial recognition systems work in practice makes opting out a near impossibility. While we do not know the mechanics of all of the wide-range of systems on the market, we do know that the StoneLock system proposed for installation at Atlantic Plaza Towers scans faces up to three feet away and if it does not recognize your face, it still takes a high resolution picture of your face and stores it in its database. Therefore, whether you consent to the use of the facial recognition system or not, the system will be tracking and collecting data on you. The KEYS Act also does not take into consideration that guests, delivery drivers, home health aides, and other individuals who may work or visit the building will be subject to this data collection, and likely will have no notice or warning that such a system is operating to collect their individual biometric data.

While we believe that an outright ban of facial recognition in the residential context would best protect LSNYC's client population and all tenants, should the City Council decide to move forward with legislation permitting the use of such technology by landlords, there is a lot more that the City could do to adequately protect tenants from harm. Measures to better protect tenants would address issues of consent, privacy protections, meaningful transparency, and continuous oversight, including the following:

a) Requirements that landlords go through a comprehensive application process that involves notice and participation by current tenants, and obtain approval by an appropriate agency prior to the installation of any facial recognition system;
b) Security standards for how biometric data is stored and protected from potential breaches;
c) Requirements that landlords disclose how the facial recognition system collects data and what data is collected;
d) Standards for data retention and what information should be purged regularly, including any information collected about non-residents;
e) Prohibitions against the use of the facial recognition system on minors under the age of 18;
f) Prohibitions against landlords sharing information collected with law enforcement;

g) Prohibitions against landlords using information collected in the context of eviction proceedings;

h) Prohibitions against landlords selling or sharing information collected with third parties;

i) Requirements that landlords obtain and disclose independent validation studies on the biometric performance relating to demographic and phenotypic characteristics, along with a process for continuous monitoring of error rates;

j) Minimum standards for biometric performance relating to demographic and phenotypic characteristics that must be met prior to installation and use;

k) Requirements that landlords procure informed consent from tenants and standards for what constitutes informed consent and penalties for retaliation against those who decline to consent;

l) Requirements that landlords provide notice to guests or any other individual visiting the building of the presence of facial recognition and any potential for data collection;

m) Requirements that landlords have alternative methods of egress should the technology fail;

n) Requirements that landlords disclose any compensation that they are receiving from the technology vendor for installation or any interest they may have in the vendor company;

o) Creation of a private right of action to anyone unlawfully subject to facial recognition; and

p) Establish remedies for data security breaches and the compromise of data.

While we do not support the practice of biometrics data collection in the residential tenancy context, we believe that additional provisions could serve to mitigate some of the potential risks and harms that tenants will face by the implementation of facial recognition technology in their homes, and make Intro No. 1672 and the KEYS Act much stronger legislative tools for advancing racial and housing justice across our City. We also believe that these bills would be strengthened by deeper and more extensive consultation with the tenant community, who are going to be most impacted by these bills, and also consultation with experts who have studied the impact and use of these technologies.

We thank you for the opportunity to give feedback on these bills and we would be happy to respond to any questions the Council may have regarding either bill.

TESTIMONY OF THE REAL ESTATE BOARD OF NEW YORK TO THE COMMITTEE ON HOUSING AND BUILDINGS OF THE NEW YORK CITY COUNCIL CONCERNING INT. 1170, INT. 1672, AND T2019-4579.

October 7, 2019

The Real Estate Board of New York (REBNY) is the City's leading real estate trade association representing commercial, residential, and institutional property owners, builders, managers, investors, brokers, salespeople, and other organizations and individuals active in New York City real estate. REBNY thanks the Council for the opportunity to testify on the use of biometric monitoring and forms of tenant access in buildings.

REBNY understands there is widespread concern about personal data and privacy. From social media hacking to sales of personal data, to data breaches, technological advances have made individuals' sensitive information available for misuse. Further concerns have been raised about the potential for these systems to discriminate against people of color. In light of these serious issues, REBNY supports efforts to develop an appropriate regulatory regime and appreciates the opportunity to help do so in the City of New York.

Biometric data systems, which detect unique human physical and behavioral characteristics, have created new opportunities with respect to building management and security. For example, it was widely reported that late this summer the New York City Police Department was able to use private building biometric systems to identify and apprehend a serial burglar from Florida. The suspect had come to New York ten times over the course of five years, breaking into homes and stealing property valued in excess of $400,000. The advanced biometric technology in private buildings greatly assisted NYPD in his apprehension.[1] REBNY recognizes the operational benefits of these advancements and hopes to see them continue.

For these reasons, regulation must strike an appropriate balance that allows for legitimate uses of these types of technologies while upholding privacy and data security while preventing discrimination. Furthermore, such local regulation must be consistent with State and Federal laws as any conflict now or in the future would prevent the City from accomplishing its goals.

BILL: Intro No. 1170-2019
SUBJECT: A Local Law to amend the administrative code of the city of New York, in relation to requiring businesses to notify customers of use of biometric identifier technology
SPONSORS: Torres, Espinal, Rosenthal, Rivera, Moya, Rose, Cornegy and Lancman

Int. 1170 would amend the New York City administrative code to require commercial establishments to place a sign or notice in a visible location near the entrance when biometric data systems are in use. The sign would inform entering customers that the businesses uses biometric data systems, identify the technology, disclose any data protection measures and whether the information is shared with third parties.

REBNY appreciates the value in informing the public when their biometric data is being collected and also believes that these monitoring and data capture technologies offer great services particularly for security in heavily trafficked entrances.

To improve the bill, we believe that greater clarity is needed in defining the circumstances in which these disclosures would be required. Specifically, while the term "commercial establishment" in the bill provides specific types of businesses offering goods and services to the public, the current language could also extend to private properties where even non-public-facing business occurs. REBNY believes the bill will be most effective if it is applied only to businesses that are directly selling goods or services to the public rather than places of business where no direct consumer transactions occur.

[1] Holcombe, Madeline. "An 82-year-old man slipped past doormen in upscale buildings for years and stole $400k in jewelry, police say." *CNN*. September 8, 2019. https://www.cnn.com/2019/09/08/us/nyc-burglar-82-years-old-upper-east-side/index.html

BILL: Intro No. 1672-2019
SUBJECT: A Local Law to amend the administrative code of the city of New York, in relation to requiring real property owners to submit registration statements regarding biometric recognition technology utilized on the premises
SPONSORS: Richards and Kallos

Int. 1672 would require real property owners that utilize biometric data systems to report the use of the technology along with information about the buildings and details about the systems to the City. The proposal would further require certain information about use of these systems in individual properties to be posted on the City's Open Data portal.

REBNY understands the Council's goals of better understanding the use of these systems in buildings across New York City. However, while certain disclosures to the City and public may be warranted, it is important to balance that priority with the legitimate security benefits provided by these systems. As drafted, the proposed legislation asks both commercial and residential buildings to reveal and publicize potentially sensitive security information that may put tenants' safety at risk. Including this information in one system serve as a virtual honeypot for hackers and other wrongdoers, potentially placing the property and tenant security at risk.

Further, Int.1672 would require all property owners to disclose the use of biometric systems including instances such systems are used to help manage those directly employed by the property (for example to assist with employee time-keeping). Requiring the registration and disclosure of systems appears to go beyond the goal of the bill.

BILL: T2019-4579
SUBJECT: A Local Law to amend the administrative code of the city of New York and the New York city building code, in relation to defining the term key and requiring building owners to provide keys to residential tenants
SPONSORS: Lander

T2019-4579 requires that all residents of buildings be given a key to their unit dwelling as well as all building entrances. The bill defines a key as a piece of shaped metal with incisions that can be put into a lock to open and close a door.

Recent instances in which keyless security systems in buildings have been installed has appropriately brought troubling situations to the fore. However, the proposed legislation would pose significant risks to the safe operations of buildings and their tenants.

Recognizing the security benefits of technology-enabled keys, many buildings have not used hard metal keys for several decades. This does not necessarily mean the use of biometric locks. Many buildings use fobs or cards with magnetic strips because, unlike metal keys, they can be easily deactivated at the end of a lease and are not easily replicated. Further, recent technology empowers the tenant to conveniently manage security in their own units. Some application-based locks give tenants the ability to remotely unlock their units to give access to service providers like dog-walkers, baby-sitters, and repair persons. Requiring all units to have a metal key would subvert all the benefits of the more advanced systems and also reduce security as having two means to open the door of a residential unit is significantly less safe.

REBNY appreciates the Council's concern for tenant access but is very concerned about requiring the installation of metal-keyed locks in all exterior entrances and that all tenants be given keys to such doors. Many residential buildings in New York City do not use a hard metal key to open and close exterior doors. This is the case because doing so would expose the building and its residents to greater risks. Metal keys can be lost and are easily replicable, both of which would potentially grant unwanted persons access to the building. If this bill were to be law, if any of the tenants in a building loses the key to the exterior door and the landlord is not notified, the safety and security of all occupants is put at risk. Moreover, some larger buildings lock certain ingress doors at night to better ensure the security of the building and tenant safety. For this reason, we believe it is inappropriate to require all buildings provide all tenants with metal keys to access all exterior doors.

Thank you for considering our views.

# # #

CONTACT(S):
Zachary Steinberg
Vice President
Policy & Planning
Real Estate Board of New York (REBNY)
(212) 616-5227
zsteinberg@rebny.com

Good afternoon council.

My name is Schuyler Duveen, representing a community group called RethinkLink.nyc. (https://rethinklink.nyc)
I've worked in the technology industry for 25 years seeing many different faces of privacy violations and the evolution into our current beyond-Orwellian state.
First as a hacker in my sophomoric high-school days, then dealing in educational and security aspects at schools, I was also Director of Technology at WNYC radio for four years.

I first want to celebrate two aspects of this bill that you should preserve with future legislation: First, you avoided the narrow framing of "facial recognition" and discuss biometric recognition in general. This is important since the industry often retreats to narrowly excluding 'facial recognition' while this is among many forms of recognition, and not even the most reliable, among others are 'gait recognition' 'voice recognition' 'smell recognition' and a recent patent filed outlines 'butt recognition'

Second, you avoid the framing of markers that immediately are connected to individuals and you define the technology around what is *capable* of identifying a person. Many times, the local company/'collector' will not know the person, but can collect markers and then pass it to other companies which do matching without any transparency that it's happening at all. The local organization can confidently say "We don't identify individuals" all the while passing biometric data to 3rd parties and targeting them or profiling them in other ways.

I'm here to request that you pass this legislation and pass further legislation that is more aggressive in the following ways:

One, that you expand identifying technology to consumer-products and objects (like key fobs) that have not been established with local permission on premises.
Our personal phones are tracked with WiFi and BlueTooth technology in all sorts of public spaces.
RFIDs are embedded in retail items to track during shipping -- from clothing to children's toys.
However, they mostly stay on beyond purchase and can often track your person while navigating public spaces carrying these items.

Secondly, that you expand the law to new york city 'furniture' -- i.e. Link.NYC kiosks.

One organization that has committed both sins above is Sidewalk labs in partnership with DoITT. Their current "privacy policy" (if you could call it such a thing) excludes "facial recognition" but doesn't say they are avoiding any other biometric markers as we walk down the street. As an example, while the privacy policy says much about how they collect video (they shouldn't be recording video at all, of course) -- they include 'audio' as "ambient noise" in a category which they can share indiscriminantly with any third parties and store indefinitely.

New Yorkers should be secure in our public space and we, the people, should set the terms for our identity being tracked rather than let the companies write their own loop-holes.

One last thing I wanted to discuss is a question that the council has asked other folks testifying today.
Besides possible the harms brought up thus far,

Credit Scores, Loan Approvals (and advertisements for opportunities) have been based on who your facebook friends are
-- these can be statistical and if collection occurs, the statistical nature allows companies to lie about how connected
these factors are -- maybe it's where I walked down the street -- or who I walked down the street with, or who visited me
in my apartment. We shouldn't wait until it becomes public that this was done.

ANHD
50 Broad Street, Suite 1402
New York, NY 10004
Tel: (212) 747-1117

TESTIMONY OF LUCY BLOCK BEFORE THE NEW YORK CITY COUNCIL
REGARDING USE OF FACIAL RECOGNITION AND BIOMETRIC DATA COLLECTION

October 7, 2019

To Chair Cornegy and members of the Committee on Housing and Buildings, the Committee on Technology, and the Committee on Consumer Affairs and Business Licensing,

My name is Lucy Block and I am the Research and Policy Associate at the Association for Neighborhood and Housing Development (ANHD). ANHD builds community power to win affordable housing and thriving, equitable neighborhoods for all New Yorkers. As a coalition of community groups across New York City, we use research, advocacy, and grassroots organizing to support our members in their work to build equity and justice in their neighborhoods and city-wide.

ANHD believes that the use of facial recognition technology and biometric data collection should be banned from New York City's residences and businesses, rather than regulated in the limited ways proposed by these three bills. We have four core concerns. First, facial recognition technology frequently misidentifies women, people of color and the elderly, creating a disproportionate risk that such residents will be locked out of their homes in the name of "security." Second, unnecessary collection of biometric data is a breach of privacy of *all* tenants, and there are no safeguards to guarantee the security of the data collected. Third, the proposed opt-out provision - though well-intentioned - cannot adequately safeguard tenants. For these reasons - and because landlords have many other, less intrusive security measures at their disposal that allow them to ensure building safety without increasing surveillance and compromising privacy - we ask that the Council reject the proposed bills and instead consider a ban on the use of facial recognition technology in housing. Such a ban is already under consideration in Albany and at the federal level, and we believe it would better serve the low-income communities of color that we work with and represent.

Discrimination is Inherent in Both the Technology and Its Proposed Roll-Out

The use of facial recognition and biometric data collection in private spaces will disproportionately disadvantage women, the elderly, and people of color, particularly those with darker skin. A 2018 MIT study showed that facial recognition software often misidentifies people of color: the authors showed that IBM's algorithm misidentifies light-skinned men just 0.3% of the time and misidentifies dark-skinned women 34.7% of the time.[1] People of color already face significant discrimination in housing, including in new luxury buildings of the sort most likely to adopt new facial recognition technology. Imagine those same residents being denied access to their home because the software does not accurately recognize dark skin tones.

Rather than ensuring the security of all residents, facial recognition and biometric data collection will add to the over-policing of residents of color in particular, while breaching the privacy of all residents. People of color are already overpoliced in public and private spaces, and artificial intelligence makes mistakes.

1 Buolamwini, Joy. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. Proceedings of Machine Learning Research 81:1–15, 2018. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; interactive website: http://gendershades.org/overview.html.

ANHD
50 Broad Street, Suite 1402
New York, NY 10004
Tel: (212) 747-1117

We cannot risk merging the two and allowing a new generation of high-tech overpolicing into our homes and businesses.

Resources:
https://www.huffpost.com/entry/facial-recognition-privacy-racism

"Security" That is Insecure

Even if facial recognition systems were free from bias, it is a serious violation of privacy for all residents, and renders *all* of their sensitive biometric information less secure.[2] CM Richards' Intro 1672 requires that landlords register their use of facial recognition technology with the DoITT. But there are no guarantees whatsoever about the security of biometric data collected – the bill does not place *any* requirements on how the data must be stored and protected or place limitations on whether and with whom landlords can share tenants' biometric information. Even if the bill had included such guidelines, no data storage system is immune to breaches and hacking. An attempt to require registration of this technology will not ensure that data is well-protected; it will not ensure the security or privacy of residents.

Tenants Will Not Be Able to Opt Out of Surveillance

We appreciate Councilmember Landers' effort to mitigate the negative impacts of facial recognition technology by seeking to require that landlords provide metal key entrances as a mandatory alternative to a facial recognition entry system and give tenants the right to opt out of the system. Unfortunately, opting out will not be a realistic option for many. First, the bill does not require affirmative consent from tenants for use of the technology, nor require landlords to alert tenants to their right to decline. Second, tenants in a tight rental market may not feel able to exercise their right to opt out if doing so many threaten their tenancy. Low-income tenants with fewer housing options will feel this pressure most acutely. Finally, even if a tenant succeeds in opting out, facial recognition entry systems may well obtain identifying information even from those who have sought to opt out. For instance, the StoneLock System proposed at APT can scan a face up to 3 feet away from the terminal, and the system takes and stores pictures of any face scanned that it does not recognize.

* * *

In conclusion, **there is no security interest that outweighs the significant potential harms of the use of facial recognition technology in residential spaces.** We urge the Council to reject these bills and instead adopt a ban on the use of this technology.

Thank you for the opportunity to testify. I am happy to answer any questions and can be reached at lucy.b@anhd.org or 212-747-1117 x13.

2 Hao, Karen. *Making face recognition less biased doesn't make it less scary*. MIT Technology Review: January 19, 2019. https://www.technologyreview.com/s/612846/making-face-recognition-less-biased-doesnt-make-it-less-scary/

Testimony of Andrew Rigie
Executive Director of the NYC Hospitality Alliance
Before the Committee on Consumer Affairs and Business Licensing
October 7, 2019

RE: Requiring businesses to notify customers of the use of biometric identifier technology

Thank you chair and members of the Committee on Consumer Affairs and Business Licensing for inviting us to testify. My name is Andrew Rigie and I am the Executive Director for the New York City Hospitality Alliance ("The Alliance"). We are a not-for-profit trade association representing restaurant and nightlife establishments throughout the five boroughs that will be impacted by **Int 1170 which would require businesses to notify customers of the use of biometric identifier technology.**

Our comments in this testimony represent general support for Int. 1170. The Alliance recognizes that technology is advancing in the hospitality industry. Business owners are utilizing tools such as data analytics and AI to improve their operations and enhance their customers' experience. While biometric identifier technology has not yet been widely adopted in the hospitality industry, we foresee that new platforms using this technology will enter the marketplace. That's why, we believe it is timely to establish clear standards and guidelines for its use.

After review of Int. 1170, we urge you to consider the following modifications:

1. The proposed legislation should clarify that "general security cameras" are not covered by Int.1170 if they only collect video footage. While many businesses have voluntarily installed general security cameras, it's important to note that businesses with a Use Group 12 Certificate of Occupancy are required by law to install video recording system. We want to make sure these businesses are not inadvertently covered by this law for using general security cameras.
2. § 20-829 a: This section should include details about where the sign must be posted by entrances. We suggest the sign is required to be posted within 10-feet in any direction from an entrance. This provision should also include a mechanism to allow the sign to be posted in an alternate location due to the design of the entryway and/or façade of building.

As new technologies enter the marketplace it's important that business owners have clear guidelines for the appropriate use of such technologies. We appreciate you considering these modifications and look forward to continuing the conversation around this topic.

Respectfully submitted,

Andrew Rigie (arigie@thenycalliance.org)

New York City Council

Committee on Housing and Buildings, Committee on Technology, and Committee on Consumer Affairs and Business Licensing

October 7, 2019

Hearing on Facial Recognition Technology and Biometric Data Collection in Businesses and in Residences

Written Testimony of Anita Booker,
Tenant of Atlantic Plaza Towers, Brooklyn, NY

As tenants of Atlantic Plaza Towers Tenant's Association (ATA), why wasn't we informed about this meeting pertaining to our place of residence? Last year DHCR sent out an owner's application for modification of services providing residents with 20 days to respond with a yes or a no, when some residents "I take that back the majority of the residents either didn't receive it or received it after the deadline because there was renovation going on in the building and the mail was tossed around. I know this because a few of us canvassed the other tenants in the lobby after a tenants meeting was held.

Tenants have so many issues that needs to be addressed, why is this such a big deal to install (which is very frightening because it's an invasion of our privacy)? People with money is starting to fixing up our neighborhoods to bring property value up, so the poor people like me can't afford to live here anymore. I am part of EBC, East Bklyn Churches and we are finding out that there are so many people are losing their homes because of the changes taken place, now we have to fight to protect our privacy, where we live. As written in the DHCR packet,

Where is the safety & security of installing this bio technology in our place of residence? Just like people walk in the building behind us when you use your key fob, what difference is it going to make if our face is scanned. The person will still come in. I have my proof that ATA security works. The five of us who was asking other tenants if they received the package from DHCR about Facial recognition, a week later we received a letter with a colored photo with our apartments written over our pictures stating that the lobby is not a place to solicit, electioneer, hang out or loiter.

Please think hard about what landlords are doing. We are not just here to speak on behalf of the tenants of ATA, with so many people needing housing, his so called affordable housing is now being designed with bio technology and people are being forced to be scanned before they sign their lease.

I ask you how would you feel as a tenant if your landlord install this gadget that would invade your privacy and you don't know where it will end up? Please help us come up with a bill to prevent this bio technology out of residential areas.

Thank you,
Anita Booker

Testimony of Fabian Rogers
249 Thomas S Boyland Street, Brooklyn, 11233

New York City Council Committee on Housing and Buildings, Committee on Technology, and Committee on Consumer Affairs and Business Licensing

October 7, 2019

Hello City Council Housing & Buildings Committee, my name is Fabian Rogers. I am a resident here on behalf of the many tenants, like those who spoke before me, of Atlantic Plaza Towers, in Ocean Hill-Brownsville, Brooklyn, and potential tenants all throughout New York City. I come to this occasion with a critical lens on the issue of the uprise of biometric surveillance & security technology in different facets of our society, because of the potential lives that can be heavily affected by these innovations. More specifically, my personal testimony is aimed at potential legislation on the table today that focuses on this type of technology's use in the housing sector, both public and private. With regards to the bills that we're engaging in discourse over, I am here to strongly suggest the idea of a moratorium on these because of the stage at which tech giants such as **Microsoft**, **IBM**, and **Face++** are at with their facial recognition technology. Although I am grateful that there are government policies being presented at all, I have to be mindful of the strength of these policies and how much protection they would provide for tenants like myself. With dealing with the vast and rapid pace of the integration of technology within our society, we have to be mindful of the consequences of dealing with new, untested, and possibly incorrectly regulated biometric technology. We have to constantly ask ourselves: what are we dealing with here? Who is affected? How are they affected? And how does that then impact the rest of society? I recommend a moratorium because although these bills mean well, I still had discomfort with the legalese of the bills proposed. I worry that despite the premise of justice in these bills, the outcome upon these bills being passed might not reach the feats of justice we hope for. That worry stems from the issue that the lives that would be most impacted have yet to truly be heard and considered. I worry that these bills would unfortunately and shrewdly fall short of providing full protection to ALL tenants in the face of unsanctioned innovation with facial recognition technology.

Interestingly enough, we often talk and focus on the steps of innovation of these emerging technologies around us. We get caught in the glamor of a new gadget that might offer a better sense of convenience in everyday activity. However, we don't think or talk as often about the missteps that come with innovation. Just like other science experiments, the hypotheses that come with these technologies can have room for errors. Typically, that margin of error is fine to tinker with and improve upon. But the major difference here is that the margin of error for facial recognition technology involves everyday people's personal biometric data. The repercussions of this type of error can cost everyday people information that the government couldn't even afford to replace. A person's biometrics is essentially priceless, and unique to them but with this

legislation, we are allowing for that private information to monetized without allowing control to the people who give up their private information in the first place. This legislation is set in a way as though we assume this facial recognition technology is full-proof when tech giants such as Microsoft, IBM, and Face++ have elusively said otherwise.

A study done by Joy Boulamwini, a researcher at MIT and Timnit Gebru, a researcher at Microsoft, through using the evaluation systems on about 2200 - 2300 facial profiles (harvested from the internet) marketed and created by Microsoft, IBM, and Face++, they found massive inaccuracies, particularly amongst the demographic of women of color. Although darker-skinned women profiles only accounted for 21% of the entire test pool of faces to evaluated, their profile accounted for 61% to nearly 73% of error rates within these same facial recognition systems being marketed by the near forerunners of this type of technology. The folks who are essentially leading the world in technological innovation in this facet, still have a large margin of error yet to be addressed. Ironically, the demographic at peril in this study is more than likely the first and main demographic at peril in reality. With gentrification phasing out the diversity in neighborhoods, these technologies will be used as surveillance tactics to essentially speed up that process, allowing landlords another metric to be an intrusion among the privacy of tenants like myself and those you heard before me.

Because there is no true regulation around these technologies, startup companies such as Stonelock, the company in the midst of trying to use their technology on the buildings which my tenants and I come from, can use their technology without necessary validation studies to show if they have actual efficacy on the data they would harvest. Think about for a second if you can, if tech giants don't have a grapple on efficacy with all demographics and startup companies may not even be required to have validation studies checked and critiqued, where does that leave the margin of error in reality? We are no longer talking about practice studies, we are talking about reality even having a worse reflection of what we've seen from information that knowledgeable data scientists have shown us time and time again. Potentially black and brown bodies who can't afford to have a voice in this battle because of everyday life challenges, can be taken advantage of and tied in to biometric data mismatches that could cost them their lives as law abiding citizens. This intrusion on personal data starts off from a premise of inaccuracy and will inherently have an outcome of heavy inaccuracy that can potentially lead to eviction, unlawful arrest, and unlawful mismanagement of people's personal data. The potentiality for people's biometric information being taken advantage of not just by landlords but by hackers exponentially grows with the uprise of starter tech companies that don't match the liking of tech giants such as Microsoft, IBM, and Face++. Thus leaving tenants like myself in a place of peril as I'm just a test subject along a bigger scheme for hasty integration of technology in our society.

New York City Council

Committee on Housing and Buildings, Committee on Technology, and Committee on Consumer Affairs and Business Licensing

October 7, 2019

Hearing on Facial Recognition Technology and Biometric Data Collection in Businesses and in Residences

Written Testimony of Icemae Gardner-Downes, Tenant of Atlantic Plaza Towers, Brooklyn, NY

Hello, I am Icemae Gardner-Downes a representative for Atlanta Plaza Towers Tenant's Association and a tenant in the building since 1968. We are here today to present our opposition to bills-INT 1672-2019 and T2019-4579.

Atlantic Plaza Towers is comprised of two 24-story buildings with a total of 714 rent stabilized units in the Brownville section of Brooklyn. It is owned by Nelson Management Group. The demographic make-up of the complex is about 80% female and minors of color.

In the fall of 2018 we received a mailing from NYS Housing & Community Renewal Office of Rent Administration/MCI unit better known as DHCR stating our owner had filed for a lease modification to install a Facial Recognition to replace the current Key Fob system. The notice instructed us to check the yes box if you agreed or check the No box and explain why you disagreed and return by given deadline. Attached to the notice was a list of every tenant's name and apartment number in your building. Privacy be dammed.

With no guidelines from DHRC we decided to:

1. organize and educate ourselves about facial recognition and biometric data technology. We "Googled" until our fingers were numb;
2. seek help from Elected Officials, Technology Experts and Brooklyn Legal Service of Brownville; and
3. we reached out to the media.

Where are we today? On May1, 21019, we filed our opposition papers with DHCR at their Jamaica office. Our State Assemblywoman Latrice Walker has since introduced Bill A7790 to prohibit the use of facial recognition system by a landlord on any residential premise. The Senate version of the same bill is S5687.

I pose these questions to City Council Members:

1. Did you speak to any experts who know about this technology before you drafted these bills?
2. Did you speak with any tenants currently living in buildings with a facial recognition system to find out about their experiences and concerns?

Because Council Members, if you had spoken to either of those groups then you would know these bills do not go far enough. We the tenants of Atlantic Plaza Towers do not believe Bills INT 1672 and T2019-4579, as proposed, are strong enough to support our opposition to the use of Facial Recognition and Biometric in residential building.

We further ask for a moratorium to stop any current or planned use of these systems until there is a full ban in place, because we know facial recognition and biometric surveillance systems have already been installed in residential buildings.

Thank you,
Icemae Gardner-Downes

City Council Committee Hearing testimony:

Hello,

My name is Tasliym Francis and I am currently a working mom, who has been raised from a 3rd generation and now raising a 4th, all rented and residing in Atlantic Plaza Towers. Alongside many of us who have lived here just as long as I have, would like to continue to raise our children in an environment where we already feel safe and secure with the many forms of security provided. This is why I am proud to be here to represent myself, Atlantic Plaza Towers tenants, and others who are in opposition for this biometric system, referred to as facial technology, and any other forms of technology that uses our biometric identity as a form of entry into a place of residence, without an option to consent. We are urging the council to broaden federal privacy legislation against the use of biometric data collection in residential buildings across NYC such as California has done, and not just for Atlantic Plaza Towers! I am testifying that we push for a moratorium and a ban on this huge imposition and since we the tenants feel that security (for reason to why Nelson Management wants this new technology in the first place) is not an issue for most of us because we face other problems that need to be address in APT. As predominately minority women raising children, now have to face an even bigger issue with the introduction of such a risky surveillance system that most tenants simply just do not want and seems to only benefits landlords, the government and private sectors. Faulty technology that would also scan the faces of our children, whose facial features changes over time, also seems to be rather problematic instead benefit to any tenants. And as some of us may know that in history when some systems have appeared beneficial to citizens, especially without proper knowledge or education, we have in fact become so unsafe that the harm-to-benefit ratio becomes inexcusable and unfair, and should be enough to bear in mind complete bans. I may sound cliché but this is an example of "everything the glitters, just is not gold". The law already prohibits certain kinds of dangerous digital technologies, such as spyware and I honestly feel that facial recognition technology can become far more dangerous, especially since hackers are still always at bay and is in dire need for prohibition in a residential building.

When entering our building we come through a door without a key, but then the next two are required the use of electronic key fobs upon entry, for a total of 3 doors. There is an intercom system, another form of electrical use; visitors enter a numerical passcode for the apartment they want to visit, and the tenant can speak back and then press a button to unlock the door. Alongside the intercom system, our cell phone numbers can be attached to this device in cases to which you do not have your key fob, we can use our cell phones to let ourselves or others into one door but not though the third door. The third door you must either have a keyfob or maybe depending who is on site, a security guard will let you in or you would have to wait for someone to come in/out. However, in any cases of emergency if a power outage happens and technology works against us, tenants and visitors would then either be locked out or in the building. Just recently, technology did failed us and there had been a power outage this past summer and left tenants without water and electricity. One building had to do without both, while one just had lacked water. Tenants from 249 had to be let in and out of the building because of no electricity for about a day and I'm quite fearful if this type of thing happens again, how long will it take to restore power? Facial recognition technology does not feel safe and I fear that in case of an emergency, strangers or just about anyone will have gain full and easier access to the property.

There's a security guard that sits in a booth, situated between the last 2 doors, watching who comes in and out of the building. After walking thru the doors, and passing a security guard, there are cameras positioned by the doors, both the front and back entry of the buildings; by the elevators, in the elevators, and as soon as we get off of the elevator to walk to our apartments…yeah you guessed it another camera! We also have a maintenance crew who also secures the premises. They are indirectly put on duty to watch us, since some were past security guards, who were given "promotions" to become a part of the maintenance team in our buildings, but some of us feel that they too, watch us. If a security guard is not sitting at the booth, a maintenance worker will be seated there. When we hang fliers up or slip them under doors, some cannot be pushed fully under the doors, we have been told that building maintenance are given strict order by management to take fliers that are visible and throw them away! Eyes are everywhere, even when we think they are not watching us, which also seems pretty frightening. When we come in or out the building with a big box, pictures have been taken of tenants which results to that tenant being investigated and/or interrogated by either sending security or one of their head maintenance, such as Mr. Moore to find out exactly what that tenant had in their box. I mean seriously to what extent do we draw the line to what is private or not? What is considered too much or too little security, especially in a low income, minority setting to where lack of privacy and consideration is given?

We as residents do not want to feel as if though we are prisoners, tagged and monitored as soon as we make a move in our homes, or in any place for that matter, particularly with a system that is ineffective. Why should we endure such treatment especially in a place where we pay our rent? Now let's take a look at Jimmy Gomez, a California Democrat, (which according to CNN, California has in fact set forth temporarily banning state and local law enforcement from using facial-recognition software in body cameras, as the largest state takes action against the technology), a Harvard graduate and one of the rare Hispanic lawmakers serving in the US House of Representatives. But to Amazon's facial recognition system, he resembled a possible criminal. Gomez was one of 28 US Congress members falsely matched with mugshots of people who've been arrested, as part of a test the American Civil Liberties Union ran last year of the Amazon Rekognition program. According to the ACLU, nearly 40 percent of the false matches by Amazon's tool, which is being used by police, involved people of color.

The results emphasizes an increasing concerns amongst civil liberties groups, lawmakers, tech firms, and even some tenants who live in buildings throughout the nation, that facial recognition could hurt minorities as the technology becomes more conventional. The usage of the technology is now being used on iPhones and Android phones, police, retailers, airports and schools are gradually approaching around to it too. With studies proving that facial recognition systems have a tougher time identifying women and darker-skinned people, which could lead to frightful false positives especially within Atlantic Plaza Towers residents, since predominately women of color living here. This is an example of how the application of technology in a residential space can cause harmful consequences for communities who are already over-surveilled.

We have experienced mere disrespect, and have been continuously treated like criminals in our own homes. For instance, when some of us first learned about facial recognition, tenants gathered in the lobby to discuss the use of this new technology. Building

management then sent the tenants who were spreading knowledge or awareness, a notice to threaten us with pictures taken from a security camera, have sent the police, and stated that the lobby was not "a place to solicit, electioneer, hang out or loiter." When in fact landlords, nevertheless, don't have the right to ban nonviolent and diplomatic gatherings in this way because it is our rights as tenants to congregate and educate one another. Our biggest danger is that this technology will get into the hands of third party entities, who will get unsolicited access to our biometric information, and ultimately we will be placed in damaging systems such as perpetual police lineups as indicated by the researchers at Georgetown Law School.

There is a huge growing gap between existing laws and current privacy bills have not been ambitious enough to protect ALL people, especially those of color & immigrants. I suggest we create a blueprint for future legislation. We need to consider ways to improve introduced bill proposals, including a central "golden rule of privacy" to ensure we can trust that our personal data is handled in ways consistent with our own interests and within the parameters in which it is collected. High-tech revolution is surpassing privacy protections. Government is now capable of collecting specifics about our private lives, for instance in New York, police have secretly installed surveillance gear planned for conflict, and now since this flawed facial recognition technology has slowly crept into transit hubs and our schools, our governments and courts have outsourced sensitive decision-making to a biased algorithm system.

According to the Medium "Tempted by this vision, people will continue to invite facial recognition technology into their homes and onto their devices, allowing it to play a central role in ever more aspects of their lives. And that's how the trap gets sprung and the unfortunate truth becomes revealed: Facial recognition technology is a menace disguised as a gift. It's an irresistible tool for oppression that's perfectly suited for governments to display unprecedented authoritarian control and an all-out privacy-eviscerating machine" and honestly I could not have said it better and I will reiterate what I stated in the beginning, that everything that glitters, just is not gold!

In Conclusion, privacy has become a complicated concept, one that frequently changes with the times and with evolving technologies. The technologies and devices one may assume as vital to modern life also keeps an extensive record of where we go, who we interact with, how we entertain ourselves, and more. As a result, we suffer the consequences and as some of us have experienced over the past several years, often corporations fail to protect our most sensitive information, by receiving unknown phone calls or unwanted emails, we are often feeling like government is secretly spying on us. There are actions one can take to secure our own information, but I still feel comfortable if broader protections requiring new legislation or even reconstructing our constitutional rights for this new digital era; since the Fourth Amendment's protection against "unreasonable" searches and seizures leaves substantial room for clarification. The urge for more privacy has been gaining recognition. Now the question is whether the courts, the federal government, or the states will step in to protect our privacy. Its future is still up for grabs.

I personally have recognized this dilemma as a new and potentially positive opportunity for Atlantic Plaza to become more engaged within our community, and to hopefully build new bonds with our neighbors, new and old, in raising awareness and setting precedents on social issues that affects not just one, but can affect us all in the future. I believe it's great

that we show that we as citizens in the United States, make strong use of our rights, and continue to voice our opinions in creating new laws that apply to a newer and a much more innovative society that which we live in.

Ladies and gentlemen, one must realize that we are living in a day and age with rapid advancement of modern technology to where artificial intelligence has become highly regulated by people in specific power, and to those who heavily depend on it for their social media or for other uses. I feel it is necessary and the wisest thing to set forth by implementing newer laws against specific advanced technology, such as facial recognition in a residential area where privacy is a huge concern and not security. Ultimately, we the tenants of Atlantic Plaza Towers already feel safe and urge our city council to push in taking better precautions against warrantless collection of sensitive data by the government, fighting for transparency about the information government sweeps up and its techniques, and advocating for New Yorkers' to cautiously take control over their personal data and who has access to it. Thank you all for your time and consideration, and I hope to hear a positive solution that makes us all happy in this case.

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1019 Res. No. 5130

☐ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: VINCENT SUTHERLAND

Address: 139 MACDOUGAL STREET, NEW YORK 10012

I represent: CENTER ON RACE, INEQUALITY AND THE LAW AT NYU SCHOOL OF LAW

Address: 139 MACDOUGAL ST, NEW YORK 10012

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1672 Preconsidered Intro Res. No. _____

☐ in favor ☒ in opposition

Date: 10/7/19

(PLEASE PRINT)

Name: Taslim Francis

Address: 216 Rockaway Avenue, Apt 10M Brooklyn, NY 11233

I represent: _____

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1672 Preconsidered Intro Res. No. _____

☐ in favor ☒ in opposition

Date: 10/7/19

(PLEASE PRINT)

Name: Anita Booker

Address: 249 Thomas S Boyland St Apt 9H Brooklyn NY 11233

I represent: _____

Address: _____

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1672 Preconsidered Intro Res. No. _____

☐ in favor ☒ in opposition

Date: 10/7/19

(PLEASE PRINT)

Name: Icemae Gardner

Address: 216 Rockaway Avenue, Apt 5E Brooklyn NY 11233

I represent: _____

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1672 Preconsidered Intro Res. No. _____

☐ in favor ☒ in opposition

Date: 10/7/19

(PLEASE PRINT)

Name: Fabian Rogers

Address: 249 Thomas S. Boyland St. Apt 17C Brooklyn NY 11233

I represent: _____

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1672 Preconsidered Intro Res. No. _____

☐ in favor ☒ in opposition

Date: 10/7/19

(PLEASE PRINT)

Name: Samar Katnani

Address: 40 Worth St. NY, NY 10013

I represent: Legal Services NYC

Address: 40 Worth St NY NY 10013

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☒ in favor ☒ in opposition to FOR of Bill

Date: 10/07/19

(PLEASE PRINT)

Name: Vanessa Bergonzoli

Address: 240 Broadway Brooklyn, NY. 11211

I represent: Tenants Association @240 Bway

Address: 240 Broadway Brooklyn, NY. 11211

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☒ in favor ☒ in opposition to FOR of BILL

Date: 10.7.19

(PLEASE PRINT)

Name: JOSH STEINBAUER

Address: 79 LORIMER STREET

I represent: NEW YORK CITY LOFT TENANTS

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: 10/7/2019

(PLEASE PRINT)

Name: Sarah Mallory

Address: _____

I represent: HPD

Address: 100 Gold

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1672 Res. No. _____

☐ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Robin Levine

Address: 2 Metrotech

I represent: DoITT

Address: 2 Metrotech 5th Flr

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☒ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Albert Fox Cahn

Address: _____

I represent: Surveillance Tech. Oversight Project

Address: 40 Rector st, NY, NY 10006

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. all bills Res. No. _____

☒ in favor ☒ in opposition

1170-2018 1672-2019

T2019-4579 *Date:* 10/7/19

(PLEASE PRINT)

Name: DANIEL SCHWARZ

Address: _____

I represent: NEW YORK CIVIL LIBERTIES UNION

Address: 125 BROAD ST, NEW YORK

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1672, 1179 4579 Res. No. _____

☐ in favor ☐ in opposition

Date: 10/7/19

(PLEASE PRINT)

Name: Laura Hecht-Felella

Address: 120 Broadway Suite 1750

I represent: Brennan Center for Justice

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1672 Res. No. _____

☒ in favor ☐ in opposition

(w/ provisos) *Date:* 10/7/19

(PLEASE PRINT)

Name: SCHUYLER DUVEEN ("SKY")

Address: 627 W113th St. #2R, NY, NY 10025

I represent: Rethink Link

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: 10/7

(PLEASE PRINT)

Name: Zach Steinberg

Address: _____

I represent: Real Estate Board of New York

Address: _____

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1170 Res. No. _____

☐ in favor ☐ in opposition

Date: 10/7/19

(PLEASE PRINT)

Name: Steven Ettannani

Address: 42 Broadway, 8th Floor

I represent: Dept. Consumer Affairs

Address: _____

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: 10/7/19

(PLEASE PRINT)

Name: CHRISTINA ZHANG

Address: 32 MONROE ST BA9

I represent: KNICKERBOCKER VILLAGE TENANT ASSOC. + AS A TENANT

Address: _____

Please complete this card and return to the Sergeant-at-Arms