NYCLU
ACLU of New York

Legislative Affairs
125 Broad Street
New York, NY 10004
212-607-3300
www.nyclu.org

Testimony of Daniel Schwarz

On Behalf of the New York Civil Liberties Union

Before the New York City Council Committee on Technology and the Committee on Civil and Human Rights Regarding the Oversight and Use of Biometric Identification Systems in New York City.

May 3, 2023

The New York Civil Liberties Union ("NYCLU") respectfully submits the following testimony regarding the oversight and use of biometric identification systems in New York City. The NYCLU, the New York affiliate of the American Civil Liberties Union, is a not-for-profit, non-partisan organization with eight offices throughout the state and more than 180,000 members and supporters. The NYCLU's mission is to defend and promote the fundamental principles, rights, and values embodied in the Bill of Rights, the U.S. Constitution, and the Constitution of the State of New York. The NYCLU works to expand the right to privacy, increase the control individuals have over their personal information, and ensure civil liberties are enhanced rather than compromised by technological innovation.

Facial recognition and other biometric surveillance tools enable and amplify the invasive tracking of who we are, where we go, and who we meet. They are also highly flawed and racially biased. The widespread use of these technologies presents a clear danger to all New Yorkers' civil liberties and threatens to erode our fundamental rights to privacy, protest, and equal treatment under the law.

The Council must ensure New Yorkers are not surveilled, targeted, discriminated against, and criminalized on the basis of invasive, flawed, and biased technology. To this end, we call for prohibitions on biometric surveillance in areas of severe power imbalance, including its use by law enforcement or other government agencies, in housing, and in other areas where our fundamental rights are at stake or where informed consent cannot be given. The NYCLU supports the two bills before the Committees, Introduction 1014-2023, which would ban biometric surveillance in places of public accommodation and set clear rules for the collection of biometric data, and Introduction 1024-2023, which would ban the use of biometric surveillance in residential buildings.

Biometric Surveillance Has No Place in New York City

Biometric surveillance technologies enable unprecedented spying powers that are dangerous when they work as advertised but also when they don't. And these technologies remain notoriously inaccurate and racially biased. Numerous studies have shown that face surveillance technologies are particularly inaccurate for women and people of color.[1] And misidentifications have led to harassments, removals from establishments, arrests, jail time, and high defense costs.[2] Each publicly known case in which a person was arrested on the basis of a facial recognition misidentification involved the wrongful arrest of Black men. And these known cases are just the tip of the iceberg. The vast majority of people will never know whether their biometrics were analyzed by a biometric surveillance system and whether such a system was involved in decisions impacting them.

The widely reported deployment of facial recognition at Madison Square Garden to ban people from the stadium that had already purchased tickets[3] illustrates the dangers from the growing surveillance industry and the urgent need for comprehensive privacy protections. And the planned installation of a facial recognition entrance system at the Atlantic Plaza Towers in Brownsville raised severe concerns about imposing invasive surveillance on residents and their guests.[4] Fortunately, the tenants were successful in their advocacy against the landlord's plan and were able to stop the system from being deployed. Such a system raises significant concerns about misidentifications resulting in potentially dangerous interactions, privacy violations by precisely tracking the coming and going of every resident and their guests, building access issues, and heightened security risks due to the collection of biometric and movement data.

[1] See e.g., Cynthia M. Cook et al., *Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*, 1 IEEE TRANSACTIONS ON BIOMETRICS, BEHAVIOR, AND IDENTITY SCIENCE 32–41 (2019); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, PROCEEDINGS OF MACHINE LEARNING RESEARCH (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[2] See e.g., Facial recognition tool led to mistaken arrest of Georgia man, lawyer says, WSB-TV CHANNEL 2 - ATLANTA (2023), https://www.wsbtv.com/news/local/facial-recognition-tool-led-mistaken-arrest-georgia-man-lawyer-says/YFV2RODJO5G4VKKJUYOBZKYROM/; Dave Gershgorn, *Black teen barred from skating rink by inaccurate facial recognition*, THE VERGE (2021), https://www.theverge.com/2021/7/15/22578801/black-teen-skating-rink-inaccurate-facial-recognition; Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, THE NEW YORK TIMES, December 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html; The Computer Got it Wrong: Why We're Taking the Detroit Police to Court Over a Faulty Face Recognition "Match," AMERICAN CIVIL LIBERTIES UNION, https://www.aclu.org/news/privacy-technology/the-computer-got-it-wrong-why-were-taking-the-detroit-police-to-court-over-a-faulty-face-recognition-match/.

[3] Kashmir Hill, *Lawyers Barred by Madison Square Garden Found a Way Back In*, THE NEW YORK TIMES, Jan. 16, 2023, https://www.nytimes.com/2023/01/16/technology/madison-square-garden-ban-lawyers.html.

[4] Erin Durkin, *New York tenants fight as landlords embrace facial recognition cameras*, THE GUARDIAN, May 30, 2019, https://www.theguardian.com/cities/2019/may/29/new-york-facial-recognition-cameras-apartment-complex.

The mere collection and storage of biometric information can also be harmful and lead to unforeseen consequences. Any database of sensitive information is vulnerable to hacking and misuse. Unlike a password or credit card number, biometric data cannot be changed if there is a security breach. And what we have witnessed so far should inspire little confidence in many companies' ability to adequately guard against misuse.[5] Disclosing data policies, setting clear retention and deletion schedules, protecting against any third-party access, and establishing appropriate security mechanisms should be the baseline for anyone handling biometric data.

Biometric Surveillance by Law Enforcement

While the two bills before the Committees focus on biometric surveillance in places of public accommodations and in residential buildings, we must stress the dangers of biometric surveillance in the hands of government agencies, specifically law enforcement. The New York Police Department ("NYPD") already has more than 20,000 cameras integrated into its Domain Awareness System[6] and plans to increase that number to a staggering 50,000 cameras.[7] And the NYPD continues to introduce even more cameras in the form of officer body-worn cameras and unmanned drones. It also makes use of social media photographs; in August of 2020, the NYPD used facial recognition software to identify a Black Lives Matter activist during a protest against police brutality through a photo from his Instagram account.[8]

Given the NYPD's long and troubling history of engaging in surveillance tactics that have targeted political dissent, criminalized communities of color, and singled out Muslim New Yorkers for suspicionless surveillance solely on the basis of their religion, the dangers that hypothetically accurate biometric surveillance technologies would pose to our most fundamental rights and liberties would be no less concerning.[9]

[5] See, e.g.: Patrick Howell O'Neill, *Data leak exposes unchangeable biometric data of over 1 million people*, MIT TECHNOLOGY REVIEW (2019), https://www.technologyreview.com/2019/08/14/133723/data-leak-exposes-unchangeable-biometric-data-of-over-1-million-people/, Josh Taylor, *Major breach found in biometrics system used by banks, UK police and defence firms*, THE GUARDIAN (2019), http://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.

[6] A Conversation with Jessica Tisch '08, HARVARD LAW TODAY (2019), https://today.law.harvard.edu/a-conversation-with-jessica-tisch-08/.

[7] Preparedness Grant Effectiveness Case Study: New York City, 27 (2021), https://www.fema.gov/sites/default/files/documents/fema_nyc-case-study_2019.pdf.

[8] George Joseph & Jake Offenhartz, *NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist's Apartment*, GOTHAMIST, Aug. 14, 2020, https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment.

[9] A few examples of the many cases the NYCLU has litigated involving NYPD surveillance abuses include *Handschu v. Special Services Division* (challenging surveillance of political activists), *Raza v. City of New York* (challenging the NYPD's Muslim Surveillance Program), and *Millions March NYC v. NYPD* (challenging the NYPD's refusal to respond to a Freedom of Information Law request seeking information about whether the NYPD is using invasive technology to infringe on the protest rights of Black Lives Matter advocates).

For more than a decade, the NYPD has deployed facial recognition in highly flawed, unscientific, and even unlawful ways. A 2019 report from the Georgetown Law Center on Privacy and Technology revealed that the NYPD engaged in such dubious tactics as uploading photographs of celebrity lookalikes in lieu of actual suspect photos, editing suspect photographs (including through effects that substantially alter the suspect's actual appearance) in order to generate a potential match, and apprehending suspects "almost entirely on the basis of face recognition 'possible matches'" without taking additional investigative steps to establish probable cause.[10]

Investigative reporters have uncovered even more failures by the NYPD to safeguard sensitive information and ensure adherence to even minimal standards on the use of biometric surveillance systems. In 2019, it was revealed that the NYPD was including mugshots of juveniles and other sealed arrest records in its facial recognition database.[11] And despite the NYPD's explicit rejection, citing concerns about security and the potential for abuse, of software developed by Clearview AI that scrapes billions of photographs from social media platforms and other public sources, it has been reported that dozens of "rogue" officers have continued to use the software in more than 11,000 searches.[12] The reporting noted that "[i]t is not clear if the NYPD officers will face any disciplinary action for using the app,"[13] raising doubts about the willingness of the police department to enforce even its own rules and raising concerns about their ability to safeguard sensitive biometric information going forward. The NYPD is far from the only agency deserving of closer scrutiny; at least 61 law enforcement agencies across New York State have secretly used Clearview AI's software, which includes more than 20 billion facial images – biometric data on virtually everyone who has ever uploaded photos to Facebook, Instagram, Twitter, Venmo, or other social media platforms.[14]

In another particularly alarming example, the Metropolitan Transportation Authority and the NYPD partnered with IBM to develop software to search for people by their skin color in the transit system.[15] And Amazon Ring has partnered with hundreds of law enforcement

[10] Clare Garvie, Georgetown Law Center on Privacy & Technology, Garbage In, Garbage Out: Face Recognition on Flawed Data, (2019), https://www.flawedfacedata.com/.

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

[12] *See, e.g.,* Craig McCarthy, *Rogue NYPD Cops are Using Facial Recognition App Clearview*, N.Y. POST, Jan. 23, 2020, https://nypost.com/2020/01/23/rogue-nypd-cops-are-using-sketchy-facial-recognition-app-clearview/; Ryan Mac, Caroline Haskins & Logan McDonald, *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, BuzzFeed News, Feb. 27, 2020, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

[13] *Id.*

[14] *See, e.g.,* Ryan Mac et al., *How A Facial Recognition Tool Found Its Way Into Hundreds Of US Police Departments, Schools, And Taxpayer-Funded Organizations*, BuzzFeed News, April 6, 2021, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition; and Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, THE NEW YORK TIMES, Jan. 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[15] George Joseph & Kenneth Lipp, *IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color*, THE INTERCEPT, Sept. 6, 2018, https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/.

agencies, including the NYPD, to facilitate data sharing from privately installed devices to the police.[16] Patents paint a dystopian vision of potential future capabilities for the home surveillance product: Business Insider reported on a myriad of concerning proposals including biometric surveillance through face, retina, iris, skin, gait, voice, and even "odor recognition"; "suspicious activity" detection; and even using the technology for "criminal prosecution."[17] Studies have shown that affect recognition and suspicious behavior detection tools overpromise on their capabilities and are severely inaccurate and plagued by racial bias.[18]

Correctional facilities have also become a testing ground for biometric surveillance technologies. The New York Department of Corrections and Community Supervision ("DOCCS") uses facial recognition for "visitation processing," deploying it to deny visitation to family members, friends, and other loved ones who wish to visit people in DOCCS's custody.[19] DOCCS has not released any information about its utilization of facial recognition for "visitation processing," and its use has not been subject to any public oversight. Additionally, DOCCS deploys a telephone system with voice recognition technology to collect and analyze voiceprints of not only the person who is incarcerated, but other parties on the call. The vendor offers investigative support, identification capabilities, call monitoring, behavioral analysis, suspicious keyword notification, pattern analysis, and even location tracking of the called party. Yet voice recognition tools have similar racial bias as other biometric technologies; studies have shown error rates for Black speakers are twice as high compared to white speakers.[20] In March 2021, it was revealed that a vendor recorded confidential attorney-client calls and provided them to New York City district attorneys.[21] An audit disclosed that nearly 2,300 calls to attorneys were recorded.[22]

[16] The NYPD is Teaming Up With Amazon Ring. New Yorkers Should be Worried | New York Civil Liberties Union | ACLU of New York, (2023), https://www.nyclu.org/en/news/nypd-teaming-amazon-ring-new-yorkers-should-be-worried.

[17] Caroline Haskins, *Amazon's Ring doorbells may use facial recognition and even odor and skin texture analysis to surveil neighborhoods in search of "suspicious" people, patent filings show*, Business Insider (2021), https://www.businessinsider.com/amazon-ring-patents-describe-cameras-recognizing-skin-texture-odor-2021-12.

[18] *See* Lisa Feldman Barrett et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements:*, PSYCHOLOGICAL SCIENCE IN THE PUBLIC INTEREST (2019), https://journals.sagepub.com/eprint/SAUES8UM69EN8TSMUGF9/full; LAUREN RHUE, *Racial Influence on Automated Perceptions of Emotions* (2018), https://doi.org/10.2139/ssrn.3281765.

[19] Beth Haroules & Lisa LaPlace, *NYCLU v. DOCCS*, New York Civil Liberties Union (2021), https://www.nyclu.org/en/cases/nyclu-v-doccs.

[20] *See e.g.*, *Voicing Erasure*, ALGORITHMIC JUSTICE LEAGUE (2020), https://www.ajl.org/voicing-erasure; Allison Koenecke et al., *Racial disparities in automated speech recognition*, 117 PNAS 7684–7689 (2020).

[21] Chelsia Rose Marcius, *NYC's 5 DA offices wound up with recordings of confidential jailhouse calls between inmates and lawyers*, NYDAILYNEWS.COM, (2021) https://www.nydailynews.com/new-york/ny-jails-recordings-attorney-client-privilege-calls-20210321-tzbyxwnle5dc5jgvi5cona6wry-story.html.

[22] Noah Goldberg & John Annese, *NYC Correction contractor recorded thousands more lawyer-client jail phone calls than first reported; could jeopardize court cases*, NYDAILYNEWS.COM, (2021), https://www.nydailynews.com/new-york/nyc-crime/ny-audit-shows-doc-listened-in-on-even-more-lawyer-inmate-calls-20211230-zni5qacdhjaozok7rdmwyg2wsm-story.html.

In the absence of federal, state, or local biometric privacy protections, private and government entities alike have been free to set their own rules for the use of biometric surveillance technologies. Unregulated facial recognition tools have been deployed and operated for far too long across agencies. We urge the Council to ban the use of biometric surveillance by police and other government entities.

Introduction 1014-2023 - Prohibiting places or providers of public accommodation from using biometric recognition technology and protecting any biometric identifier information collected.

Intro. 1014 would amend the biometric disclosure for businesses law (Local Law 3 of 2021), Section 22-1201 of the Administrative Code, to prohibit places or providers of public accommodations from using biometric recognition technology to identify customers, and it would require written consent for any collection of biometric identifier information. It would further create transparency, security, and deletion requirements and ensure that customers are not treated or charged differently because they do not consent to the collection of their biometric data.

These changes add crucial protections to New York City law. As mentioned above, the deployment by MSG Entertainment across its sports and entertainment venues to target staff from law firms in litigation with MSG points to Orwellian use cases where it will be impossible to move and associate freely. And the technology's racial as well as gender bias risks disproportionately impacting women and people of color, such as in the misidentification of a Black teenager that barred her from entering an ice-skating rink.[23] For these reasons, we support banning biometric surveillance in places of public accommodations. Furthermore, visiting retail stores, restaurants, museums, entertainment venues, or healthcare sites should not automatically open one up for the collection of sensitive biometric information without prior informed consent and clear rules for access, use, security, retention, and deletion.

While Local Law 3 of 2021 was a modest first step in addressing use of biometric technologies by businesses, it was nowhere near sufficient. That law merely requires certain "commercial establishments" that collect, use, or retain "biometric identifier information" from their customers to post signs at all entrances. The minimal notice does not include any information about the specific biometric surveillance tools in use or the collected data and further does not require businesses to disclose for what purpose the technology is used, for how long data is retained, with whom data is shared, or how it is secured. The NYCLU has repeatedly testified on this issue at the committee hearing on October 7, 2019, the hearing by the Department of Consumer and Worker Protection on the proposed rules on August 30, 2021, and the Committee on Consumer and Worker Protection on February 24, 2023. In addition to its

[23] Dave Gershgorn, *Black teen barred from skating rink by inaccurate facial recognition*, THE VERGE (2021), https://www.theverge.com/2021/7/15/22578801/black-teen-skating-rink-inaccurate-facial-recognition.

important ban on the use of biometric recognition technologies in places of public accommodations, Introduction 1014 would create the needed guardrails and protections for any biometric identifier information that such places of public accommodation may still be permitted to collect. To ensure that the legislation fully meet its goals, we make the following recommendations.

The proposed text still defines “biometric identifier information” with respect to information that is “used by or on behalf of a commercial establishment.” The bill, however, would remove the definition of the term “commercial establishment” from the statute. We therefore suggest removing “by or on behalf of a commercial establishment” in order to ensure conformity with the surrounding language.

Similarly, the definition of "customer" remains tied to the to-be-deleted term of “commercial establishment.” Instead of merely editing or removing the mention of this term, we recommend utilizing “individuals,” “natural person,” or other broader and more inclusive terms appropriate for the context in public accommodations throughout the entire bill instead of the narrower term of “customer.”

Section 22-1202 subdivision (d.) creates the important requirement for providers or places of public accommodations in possession of biometric identifier information to develop written policies with respect to their retention and use and further requires that these policies be made available to the public “upon request”. The Council should mandate that these policies be made publicly available outright, rather than conditioning their availability on a request. Transparency is key here and putting the burden on affected people to first request the policy risks subjecting them to significant time delays or accessibility hurdles, thus creating unnecessary barriers that should be mitigated up front.

Finally, Section 22-1203 amends the existing private right of action of Local Law 3, which requires prior notice of at least 30 days to violating entities, allowing them to cure the violation within 30 days to prevent further action. Although the amendment ensures that an aggrieved person would not have to provide such notice prior to commencing an action against a place or provider of public accommodation that uses a prohibited biometric recognition technology or that shares, sells, or discloses biometric identifier information, the legislation would require those who have been subject to unconsented biometric data collection to first inform violating entities and allow them 30 days to cure the violation. Such an obligation severely undermines the proposed affirmative written consent protection. The importance of a robust private right of action as an accountability and enforcement tool cannot be overstated, and we strongly urge the Council to strengthen this section to protect against violations.

The NYCLU supports this legislation and urges its passage.

Introduction 1024-2023 - Limiting the use of facial recognition technology in residential buildings.

Intro. 1024 would prohibit owners of multiple dwellings to install, activate, or use any biometric recognition technology that identifies tenants or their guests. Such strict limits are necessary because the deployment of biometric surveillance at people's homes raises constitutional concerns and intrudes on tenants' rights of self-determination and privacy. It risks conditioning entry into one's home – the place where our constitutional rights are at their most robust – on the provision of one's most sensitive biological data. Residents should not have to live in fear that landlords are tracking their comings and goings and amassing sensitive data on them and their guests. And those tenants and guests who are women, children, and people of color have particular reason to fear such a change in their housing rights, as facial recognition systems are notoriously inaccurate when it comes to these groups. Thus, not only does biometric surveillance in residential buildings cause harm to tenants' privacy rights, but also their civil rights to access housing on equal and nondiscriminatory terms.

Notably missing from the bill is a private right of action that would provide tenants and their guests with a tool to hold landlords accountable. Without it, there would be no recourse for affected people and likely no enforcement against violating landlords. Given the City's housing crisis, we strongly recommend the addition of a private right of action as a crucial enforcement and accountability mechanism.

This legislation would make clear that invasive biometric surveillance has no place in New York City housing. It would ensure tenants' privacy rights and their civil rights to access housing on equal and nondiscriminatory terms are protected. We support this bill and call for its passage by the Council.

Conclusion

In conclusion, the NYCLU thanks the Committees on Technology and on Civil and Human Rights for the opportunity to provide testimony and for their oversight of biometric surveillance in New York City. Nobody wants to live in world where pervasive surveillance identifies them, tracks their movements and associations, and impacts which places they can visit, which services they can access, with whom they meet, or how they exercise their free speech rights. The NYCLU supports Introductions 1014-2023 and 1024-2023 and we urge their swift passage.