ACLU of New York

Legislative Affairs
One Whitehall 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 Consumer and Worker Protection Regarding the Oversight of Facial Recognition Technology in New York City Businesses.

February 24, 2023

The New York Civil Liberties Union ("NYCLU") respectfully submits the following testimony regarding the oversight of facial recognition technology in businesses. 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.

In recognition of these harms, the New York City Council enacted Local Law 3 of 2021 as a first step to respond to the spread and use of these surveillance technologies in businesses. As we have stated in our prior testimonies and further below, the law takes a rudimentary approach to biometric surveillance technology, solely requiring businesses to post signs advising that biometric data is being collected but without requiring the provision of adequate information about the type of surveillance or the policies guiding its use. It is imperative to create meaningful privacy protections that, at a minimum, require informed opt-in consent, set clear limits on retention, use, and sharing, and explicitly ban the use of biometric surveillance in areas of severe power imbalance, such as when used by law enforcement, in housing, in employment, and in other areas where our fundamental rights are at stake.

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, and jail time.[2]

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.

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.[4] Disclosing data policies and creating appropriate security mechanisms should be the baseline for anyone handling biometric data.

While the focus of this hearing is on facial recognition in businesses, we must stress the dangers of biometric surveillance in the hands of government agencies. The New York Police Department ("NYPD") already has more than 20,000 cameras integrated into its Domain

---

[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] 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.

Awareness System[5] and plans to increase that number to a staggering 50,000 cameras.[6] 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.[7]

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.[8]

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.[9]

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.[10] 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

---

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

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

[7] 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.

[8] 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).

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

[10] 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.

the software in more than 11,000 searches.[11] The reporting noted that "[i]t is not clear if the NYPD officers will face any disciplinary action for using the app,"[12] 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.[13]

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.[14] And Amazon Ring has partnered with hundreds of law enforcement agencies, including the NYPD, to facilitate data sharing from privately installed devices to the police.[15] 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."[16] Studies have shown that affect recognition and suspicious behavior detection tools overpromise on their capabilities and are severely inaccurate and plagued by racial bias.[17]

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

---

[11] *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.

[12] *Id.*

[13] *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.

[14] 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/.

[15] 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.

[16] 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.

[17] *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.

members, friends, and other loved ones who wish to visit people in DOCCS's custody.[18] 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.[19] In March 2021, it was revealed that a vendor recorded confidential attorney-client calls and provided them to New York City district attorneys.[20] An audit disclosed that nearly 2,300 calls to attorneys were recorded.[21]

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. While Local Law 3 of 2021 was a first step in addressing use of these technologies by businesses, it is 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 during the committee hearing on October 7, 2019, and the hearing by the Department of Consumer and Worker Protection on the proposed rules on August 30, 2021. We urge the Council to establish the guardrails needed to protect against biometric surveillance technologies, which, at a minimum, requires informed opt-in consent, clear limits on use, access, sharing, and retention, and mandatory security standards.

A state bill, the Digital Fairness Act, S.2277/A.3308, introduced by Assemblymember Cruz and Senator Kavanagh, serves as model legislation for comprehensive privacy protections and would ensure our anti-discrimination laws and civil rights are not circumvented by digital means, prevent surreptitious surveillance, and create urgently-needed biometric privacy protections akin to the Illinois Biometric Information Privacy Act (BIPA). Enacted in 2008,

---

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

[19] *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).

[20] 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.

[21] 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.

BIPA stood the test of time, clearly illustrating there's no substitute for individual, informed opt-in consent. It continues to offer crucial biometric protections that affect Americans far beyond the state of Illinois. Powerful examples include the success against unchecked facial recognition by Facebook and, more recently, the Clearview AI settlement that – amongst several other restrictions – prohibits the vendor from offering their invasive product to private entities.[22]

In conclusion, the NYCLU thanks the Committee on Consumer and Worker Protection 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, or how they exercise their free speech rights. We urge the Council to take action that meet these values and put an end to ever-expanding surveillance across the City.

[22] In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law, AMERICAN CIVIL LIBERTIES UNION (2022), http://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois.