Testimony of Assistant Commissioner Carlos A. Ortiz
New York City Department of Consumer and Worker Protection

Before the Committee on
Consumer and Worker Protection

Hearing on Introduction 8

February 24, 2023

Introduction

Good morning, Chair Velázquez and members of the Committee on Consumer and Worker Protection. My name is Carlos Ortiz, and I am the Assistant Commissioner for External Affairs at the Department of Consumer and Worker Protection (DCWP). Thank you for the opportunity to testify today on Introduction 8, relating to the disclosure of service fee charges for tickets to entertainment events in New York City.

DCWP and Pricing Disclosures

When it comes to price transparency, DCWP is committed to leading efforts to protect New Yorkers. One of the main ways that DCWP does that is by enforcing the Consumer Protection Law, which prohibits illegal trade practices like deceptive advertising that prey on consumers. DCWP also enforces protections governing disclosures of refund policies, layaway plans, and the sale of secondhand items.

Businesses may at times hide costs to consumers by tacking on a variety of fees, such as service or processing fees, to an initial product price. The consumer may only find out the true cost of an item at the end of a transaction. This "drip pricing" approach is frustrating for consumers and can make it harder for them to budget for their purchases.

Over the years, DCWP has supported regulatory initiatives to promote price transparency and reduce junk fees on the state and federal levels. In 2022, New York State passed a law that requires operators, ticket platforms, and ticket resellers to disclose the total cost of a ticket prior to the ticket being selected for purchase.[1] The Consumer Financial Protection Bureau (CFPB) also launched a federal initiative to reduce or eliminate junk fees, such as overdraft or non-sufficient fund fees, which cost Americans billions of dollars annually.[2] Likewise, other federal agencies such as the Federal Trade Commission and the Department of Transportation have recently pursued rule changes to crack down on junk fees and increase price disclosures.[3] DCWP has submitted comments in support of these and other similar efforts to ensure price transparency at the local level.

[1] https://legislation.nysenate.gov/pdf/bills/2021/S9461

[2] https://www.cnbc.com/2022/10/26/consumer-watchdogs-new-guidance-aims-to-end-junk-fees-at-banks.html

[3] FTC: https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-proposes-rule-ban-junk-fees-bait-switch-tactics-plaguing-car-buyers; DOT: https://www.transportation.gov/airconsumer/AirlineAncillaryFeeNPRM.

Introduction 8

Turning to today's legislation, Introduction 8 would require event operator to disclose service fees, along with the price of a ticket, on advertising and promotional materials. DCWP supports this bill and believes it will lead to greater price transparency in the entertainment sector.

DCWP recommends expanding the scope of this bill to also require the disclosure of the full price of tickets at the time of sale. This change would ensure that consumers are aware of what they are going to pay for an entertainment event from its promotion to the moment of purchase. We look forward to working together with the Council on this bill as it progresses through the legislative process.

Conclusion

Thank you again for the opportunity to testify today about the disclosure of service fee charges for entertainment tickets, a problem that New Yorkers know all too well. I look forward to any questions you may have.

STATE SENATOR BRAD HOYLMAN-SIGAL
Senate District 47
322 Eighth Avenue
New York, NY 10001
T. (212) 633-8052
F. (212) 633-8096

STATE ASSEMBLY MEMBER TONY SIMONE
Assembly District 75
214 West 29th Street
New York, NY 10001
T. (212) 807-7900
F. (212) 243-2035

Testimony of State Senator Brad Hoylman-Sigal and State Assembly Member Tony Simone to the New York City Council Committee on Consumer and Worker Protection Regarding the Use of Facial Recognition Technology by New York City Businesses

February 24, 2023

Thank you for the opportunity to submit testimony to the New York City Council regarding the use of facial recognition technology by New York City businesses.

State Senator Brad Hoylman-Sigal represents the 47th Senate District, which runs from Stonewall Inn to 103rd Street along Eighth Avenue, and includes part of Madison Square Garden. Assembly Member Simone represents the 75th Assembly District, covering much of the same area.

In the Senate, Senator Hoylman-Sigal carries multiple bills regulating the use of facial recognition technology. We are deeply concerned about the growing use of facial recognition software in public spaces by private entities. We are grateful to the Council for considering this weighty issue.

Facial recognition technology has been proven to be inaccurate and discriminatory and can lead to the misuse of personal biometric data without consent. A 2019 analysis by the National Institute of Standards and Technology of 189 facial recognition algorithms — the majority of the industry — found that this technology erroneously identifies Black and Asian faces 10 to 100 times more often than it does white faces. The report also discovered that women, the elderly, and children, too, were more likely to be falsely identified. These discriminatory failures overlap. Women of color, and particularly young Black women, have some of the poorest identification accuracy rates of any demographic.

Other research has found that these algorithms also misidentify trans men as women 38% of the time, and non-binary people 100% of the time. The technology also poses grave privacy concerns, as individuals' face information is usually collected without their consent, cannot be encrypted, and is therefore vulnerable to data security breaches.

For all these reasons, facial recognition software should be used sparingly and cautiously. And yet, facial recognition technology is already being deployed in an array of concerning contexts.

For example, members of this committee may be aware of recent controversy around Madison Square Garden Entertainment's disturbing use of facial recognition software to identify and eject patrons from their entertainment venues who they deem to be hostile to the legal or financial interests of MSG. MSG Entertainment has repeatedly deployed this tech against attorneys who represent clients suing MSG — and even against people working at the same firms who have nothing to do with those cases.

This practice is deeply worrying because it sets a precedent of private companies chilling free speech by denying access to those that disagree with MSG's owner, James Dolan. This policy also violates the privacy of entertainment patrons, who have no idea their biometric information is being collected on a casual sports outing.

This policy is clearly not about public safety. This is retaliation against MSG's perceived legal enemies, chilling speech and access to the courts. Where does this end? Journalists? Labor? Banning someone from going to their local grocery store? James Dolan, the owner of MSG Entertainment, says the Garden can do whatever it wants because it's on "private property" and that MSG has a right to "defend itself." To that we say: if it's your private property, why don't you pay property taxes on it? New Yorkers subsidize Madison Square Garden to the tune of $43 million every year via tax breaks. So New York taxpayers are directly funding these abusive tactics.

Facial recognition technology allows MSG Entertainment to retaliate and potentially discriminate at a scale that would not be possible without the technology. This flawed technology and the manner in which it is deployed is an attack on all of our privacy and civil liberties.

MSG has refused to change its facial recognition practices in response to our and other elected officials' requests. That's why Senator Hoylman-Sigal has introduced a bill to add sporting events — like Knicks games — to the long-standing law that prohibits wrongful refusal of admission in places of public entertainment. It's already illegal to deny admission to Broadway musicals, public talks, and concerts. But there's a loophole in New York's statute that exempts sporting events from this rule. The senator's bill would close that loophole and make it clear that banning people from any public event is not acceptable in New York.

We thank the committee for investigating this use of facial recognition by private businesses, and would urge you to also investigate and highlight similarly problematic uses which we are also hoping to address in Albany, such as the use of facial recognition by law enforcement and residential landlords. Landlords already wield significant power over tenants by controlling their access to stable housing. Installing a facial recognition system on residential premises and then requiring tenants to consent to the use of such a system to remain in the building is tantamount to evicting those who object to having their sensitive personal data stored and used by a landlord. Senator Hoylman-Sigal is also considering legislation that would ban the use of biometric technology more broadly from places of public accommodation.

Thank you for the opportunity to speak today. We are hopeful that we can make progress on this issue on the state level, and we appreciate your partnership in addressing these harms on the city level as well.

PUBLIC ADVOCATE FOR THE CITY OF NEW YORK

Jumaane D. Williams

TESTIMONY OF PUBLIC ADVOCATE JUMAANE D. WILLIAMS TO THE NEW YORK CITY COUNCIL COMMITTEE ON CONSUMER AND WORKER PROTECTION

FEBRUARY 24, 2023

Good afternoon,

My name is Jumaane D. Williams, and I am the Public Advocate for the City of New York. I would like to thank Chair Velázquez and the members of the Committee on Consumer and Worker Protection for holding this hearing.

Fundamentally, New Yorkers are protected by the First Amendment's right to privacy. Individuals should expect that they can freely conduct private transactions without being surveilled. To that end, in 2021 my office partnered with then Borough President Gale Brewer, Amnesty International, S.T.O.P, and AI For the People on a Ban the Scan campaign, raising awareness of the dangers of public and private use of facial recognition AI. At that time I asked the previous administration to 1- Cease use of all facial recognition technology, 2 - Permanently destroy data collected and used for facial recognition in the past, and 3 - Publish data concerning each instance in which facial recognition technology was utilized.

Through non-consensual data capture, businesses violate the right to privacy. Individuals should not be removed from a place of business, because their employer is involved in legal action against said business. Especially when the business engages in its trade, in the case at hand—selling tickets to events, and then reneges to allow the purchaser/employee to redeem the ticket they purchased. The employee is not involved in the litigation. If any business could monitor and remove people because of a grievance against an employer or someone they have a relationship with, it would mean a world where businesses have the right to bar anybody from any establishment based on a tangential connection. Moreover, there was another instance where a parent was denied entry to an event on a school trip in which they were serving as an escort. This act created safety risk for the children as well as creating a stressful situation for the other adult who had to care for more children on their own.

Furthermore, citizens should not be photographed, recorded, and have personal information scanned without any repercussions. In today's economy, privacy is highly valuable. As our data broker economy continues to grow, there must be measures in place to protect New Yorkers' privacy. It is unclear today whether facial recognition software used in private businesses is also selling the information to data brokers.

While there are security concerns that impact the decision making of private businesses, the City of New York cannot let businesses broadly use facial recognition technology and run afoul of everyone's right to privacy as granted under the U.S. Constitution. It is important to note the many documented instances of facial recognition technology having racial and gender biases. Researchers at MIT reported in January[1] 2019 reported that facial recognition software marketed by Amazon misidentified darker-skinned women 31% of the time, while others have *"shown that algorithms used in facial recognition return false at a higher rate for African Americans than white people unless explicitly recalibrated for a black population.*[2]" Specifically, the technology misidentifies people with dark complexions 15% of the time as compared to only 3% for people with light complexions[3]. These findings prompted experts at Google, Facebook, and Microsoft to sign a letter calling on Amazon to stop selling its facial-recognition technology to law enforcement[4].

One final note, facial recognition technology is only one of several biometrics technologies being developed for identification purposes. Others include Long-range cardiac signature detection, Gait analysis, and an Iris scan. We must engage in discussions now on how to address and prevent the use and abuse of all these technologies. Thank you.

[1] https://www.technologyreview.com/2019/01/29/137676/making-face-recognition-less-biased-doesnt-make-it-less-scary/

[2] https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html

[3] Ibid 1

[4] https://medium.com/@bu64dcjrytwitb8/on-recent-research-auditing-commercial-facial-analysis-technology-19148bda1832

NYCLU
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.

THE BROADWAY LEAGUE®

729 Seventh Avenue, 5th Floor New York, NY 10019
212-764-1122 www.BroadwayLeague.com

STATEMENT OF THE BROADWAY LEAGUE
CONCERNING NEW YORK CITY COUNCIL INTRO 8

February 24, 2023

The Broadway League has been the principal trade association for the commercial theatre industry in New York State and across North America for over 90 years. It presently represents more than 700 theatre owners, producers and road presenters nationwide – with a majority maintaining offices in New York City.

We would like to recognize Chairperson Velazquez and the other distinguished members of the Consumer and Worker Protection Committee, as well as Councilman Brannan and the other sponsors of Intro 8 for holding this meeting and your ongoing efforts to address consumer protection issues facing our City's ticket buyers. Each year, Broadway hosts millions of travelers from around the globe. Of the approximately 14.8 million Broadway tickets sold in the theatre season ending May 2019 (the last full season before the COVID-mandated shutdowns), approximately 35% were bought by patrons from the New York City metropolitan area, while 65% were purchased by tourists (46% from outside New York City and its suburbs, and 19% from foreign countries). Broadway's cumulative fiscal impact on New York City during that period was $14.7 Billion derived from audience spending, show investment, capital improvements and operating expenses. Collectively, Broadway supported approximately 96,900 jobs, including actors, directors, ushers, electricians and publicists -- the majority of which are unionized.

Given that the State Legislature recently examined this issue in great detail in consultation with many stakeholders, including the Broadway League, through revisions to the New York State ticket resale law signed into law in 2022 that expire in 2025, we strongly recommend that the Council defer to State law at this time without introducing further changes and additional complexity. The League has always strongly supported transparency in the ticket-purchasing process to ensure that consumers are aware of the source, price and fees associated with their purchases. During last year's discussions, we advocated for State lawmakers to implement improved consumer protections, including enhanced market transparency for all tickets sold to live events. Under a State Law passed in 2018, online ticket resale sites were required to disclose "in a clear and conspicuous manner" the total price of the ticket -- and how much of that is made up of service charges -- before a sale was completed. More recently, Governor Kathy Hochul signed several additional amendments into law on June 30, 2022, including a mandate that all ticket sellers provide the total cost "displayed in the ticket listing prior to the ticket being selected for purchase."

Accordingly, we would propose the Council allow ticket providers sufficient opportunity to comply with the new State mandates before evaluating whether additional regulation may be necessary. Intro 8 introduces significant compliance challenges with respect to digital advertising, open-ended runs with varying ticket prices (as is common for Broadway), multiple distribution outlets, promotions and dynamic pricing. Implementing these changes while Broadway is still struggling to return to pre-pandemic ticket sales levels would be extremely challenging.

We are grateful that the City Council continues to take an active interest in the health of the live entertainment industry. We maintain, however, that State law satisfactorily addresses concerns about consumer cost awareness and that the changes made to State law in 2022 should have time to play out before the City advances further alterations to the sale of tickets for live entertainment. Thank you for this opportunity to express our concerns.

Good morning. My name is Leila Nashashibi, and I am speaking on behalf of Fight for the Future in support of policy to ban facial recognition to protect consumers and workers.

Fight for the Future is a digital rights organization, with over 2.5 million members nationwide, including over 85,000 in New York City. Among other focuses, we are a leader in the fight to ban facial recognition.

We're reeling at the news that the owner of iconic New York City venues Madison Square Garden and Radio City Music Hall is using facial recognition to identify, harass, and ban people from his venues. It's a disturbing example of what's possible when powerful, vengeful people get ahold of advanced surveillance technology tools, and represents a watershed moment that should concern anyone that cares about the privacy and safety of workers, performers, and consumers.

At Fight for the Future, we believe facial recognition is much more like biological weapons than alcohol or tobacco: the severity and scale of harm that facial recognition technology can cause requires much more than a regulatory framework - it requires a full-on ban.

In terms of its impact on workers, facial recognition is an Orwellian tool that allows for constant surveillance of employees, which can result in unfair hiring and disciplinary actions, often disproportionately harming Black and brown workers.

I'd like to mention some specific examples of how this tech is impacting people working at businesses:

- Corporations are using facial recognition on workers in hiring, to replace traditional timecards, and to monitor workers' movements and "productivity"
- Uber Eats drivers have been fired because of the company's faulty facial identification software, which requires drivers to submit selfies to confirm their identity. When the technology isn't able to match photos of the drivers with their accounts, drivers get booted off the system and are unable to work, and thus unable to pay their bills.
- Amazon delivery drivers have to agree to AI surveillance, including facial identification, or else lose their job

This level of surveillance is a violation of people's rights on so many levels, and is putting them in an impossible position: give up your most sensitive biometric data, your privacy, and submit to being tracked, or go unemployed. We can also be sure it will suppress worker efforts to organize and engage in collective action.

For consumers, facial recognition is able to track peoples' every move and create a digital map of where people go, what they buy, and who they interact with. Not only is this a huge invasion of privacy, but this data can also be used to manipulate consumers through personalized advertising, convincing them to buy products they wouldn't otherwise buy, and the data can be shared with other companies or law enforcement agencies. Because of the lack of laws protecting people from FRT, there is also generally no way for people to know if they are under this surveillance and no way to avoid it. Many of these systems say they pick up on "abnormal movements" as they track people, which puts neurodivergent people and people with physical disabilities at risk of being flagged and harassed or accosted by security guards.

Stores are also already using FRT to scan people's faces and can bar entry to anyone who gets matched, for example, to a mugshot database. We know that because of the reality of over-policing and the prison industrial complex that targets Black and brown communities, Black and brown people are severely over-represented in these databases. It's basically outright discrimination, and it's legal. It's very easy to imagine additional ways this tech will be used by business owners to target entire groups of people and keep them out of their stores.

A previous panelist suggested it's more dangerous to have your Social Security Number stolen than your facial recognition data, and we strongly refute that assertion. For starters, biometric data can't be replaced if stolen. That means that once identity thieves and hackers have the data, they have it for life. Secondly, there is broad consensus among security experts that stolen data can be used to access private online accounts or other information, and to stalk and harass people.

The only solution that will truly protect people's safety and privacy is to ban government and private use of this tech. When it comes to addressing businesses' use, we urge New York city to follow the lead of Portland, Oregon, the first city in the nation to pass a ban on facial recognition in all places of public accommodation.

Right now we're at a crossroads - a pivotal moment in history. We have to ask ourselves: do we want a society controlled by authoritarian forces where people are constantly being watched and policed, or do we want a society in which everyone's human rights are protected, and everyone's safety matters?

It's time for elected officials to draw a line in the sand and put an end to the spread of this tech. The decisions that we make about technology and the policies that govern it are going to shape not just the next 10 years, but the entire future of human civilization. The stakes are really that high. Thank you.

GEORGETOWN LAW
Center on Privacy & Technology

Written Testimony of

Meg Foster, Justice Fellow

Center on Privacy & Technology at Georgetown Law

Before the

New York City Council
Committee on Consumer and Worker Protection

Hearing on

Oversight - The Use of Facial Recognition Technology in New York City Businesses

Friday, February 24, 2023

For more information, contact Meg Foster at meg.foster@georgetown.edu.
Chairperson Velázquez and Members of the Committee,

I am submitting this written testimony on behalf of the Center on Privacy and Technology at Georgetown Law. We respectfully urge the Committee, and eventually NYC Council, to pass legislation to end the use of facial recognition technology in NYC's public and private sectors.

The Center on Privacy & Technology at Georgetown Law is a law and research think tank that focuses on the privacy rights and surveillance of historically marginalized communities. Its track record includes rigorous, long-term research and groundbreaking legal and policy analysis and advocacy, resulting in state and federal legal reforms to protect vulnerable people's civil rights and liberties from both government and corporate surveillance.

The Center has been studying face recognition since its founding in 2014. In 2016 we published *The Perpetual Line-Up*,[1] the first comprehensive report on how law enforcement agencies across the country use face recognition technology. Since then, we have published four more major reports,[2] testified before the United States Congress and numerous state legislative bodies,[3] and worked alongside civil society and community organizations to expose and advocate against the harms of facial recognition technology, including its threats to civil rights and liberties.

While the use of facial recognition technology by private businesses has drawn "new criticism" amid Madison Square Garden Entertainment's ("MSG Entertainment") policy of banning

[1] Clare Garvie, Alvaro Bedoya and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Center on Privacy & Technology at Georgetown Law (October 18, 2016), https://www.perpetuallineup.org.

[2] *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Center on Privacy & Technology at Georgetown Law (May 16, 2019), https://www.flawedfacedata.com; Clare Garvie and Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, Center on Privacy & Technology at Georgetown Law (May 16, 2019), https://www.americaunderwatch.com; and Harrison Rudolph, Laura M. Moy & Alvaro M. Bedoya, *Not Ready for Takeoff: Face Scans at Airport Departure Gates*, Center on Privacy & Technology at Georgetown Law (December 21, 2017), https://www.airportfacescans.com; Clare Garvie, *A Forensic Without a Science: Face Recognition in U.S. Criminal Investigations*, Center on Privacy & Technology at Georgetown Law (December 6, 2022), forensicwithoutscience.org.

[3] *See, e.g.*, Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties: Hearing Before the H. Comm. on Oversight and Reform, 116th Cong. (2019) (Statement of Clare Garvie, Senior Assoc., Center on Privacy & Technology at Georgetown Law), https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-GarvieC-20190522.pdf; Facial Recognition Technology Use: Hearing Before the Utah State Legislature Government Operations Interim Committee (2019) (Statement of Harrison Rudolph, Assoc., Center on Privacy & Technology at Georgetown Law), https://le.utah.gov/av/committeeArchive.jsp?mtgID=16538&timelineID=144852; Hearing on S. 1385, An Act Establishing a Moratorium on Face Recognition and Other Remote Biometric Surveillance Systems, and H. 1538, An Act Relative to Unregulated Face Recognition and Emerging Biometric Surveillance Technologies, Before the Massachusetts Legislature Joint Comm. on the Judiciary (2019) (Statement of Jameson Spivack, Policy Assoc., Center on Privacy & Technology at Georgetown Law), https://malegislature.gov/Reports/9783/263.pdf.

lawyers employed by firms engaged in active litigation with the company[4] (a policy made widely known by the ejection of a mother who was accompanying her daughter's Girl Scout troop to a Rockette's show in December,[5] and owner James Dolan's subsequent doubling down on this retaliatory or censorial use of the technology[6]), MSG Entertainment has been employing facial recognition at its venues since 2018 and it is one of over 200 private companies that had accounts with facial recognition software company Clearview AI as of 2020.[7] Thus, it is well past time for oversight. In today's testimony, I hope to make three points that should inform your investigation of and response to the use of facial recognition technology by business owners in New York City.

- First, left unregulated, companies can and will use facial recognition technology to retaliate against people whose speech and advocacy they find displeasing. This not only harms expressive freedoms, but it also has the potential to undermine public health and safety and to impede meaningful competition.
- Second, private actors can use facial recognition technology to discriminate, either directly by using the technology to identify and exclude members of protected groups or people who disproportionately belong to those groups, or indirectly by basing identification and exclusion policies on proxies that closely correlate with those groups.
- Third, existing law is inadequate to mitigate the pervasiveness of facial recognition technology, the risk that users will abuse it, and the breadth of harm that flows from such abuse.

A. Business Owners Can Use Facial Recognition Technology to Punish Adversaries.

As the incident(s) at MSG Entertainment suggest, private business owners can and do utilize facial recognition technology to engage in retaliation, and the potential chilling effect of this use is obvious. As New York State Attorney General Letitia James suggested in a recent letter to MSG Entertainment regarding its facial recognition policy, "forbidding entry to lawyers representing clients who have engaged in litigation against [MSG] may dissuade such lawyers from taking on legitimate cases, including sexual harassment or employment discrimination

[4] Anna Lucente Sterling, *Facial Recognition Tech Draws New Criticism Amid MSG Controversy,* NY1 (February 15, 2023), https://www.ny1.com/nyc/all-boroughs/news/2023/02/14/facial-recognition-tech-draws-new-criticism-amid-msg-controversy.

[5] Kashmir Hill, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, New York Times (December 22, 2022), https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html.

[6] Jake Offenhartz, *MSG CEO James Dolan Has 'Meltdown' about Facial Recognition Criticism, Vows to Keep Scanning Opponents*, Gothamist (January 26, 2023), https://gothamist.com/news/msg-ceo-james-dolan-has-meltdown-about-facial-recognition-criticism-vows-to-keep-scanning-opponents.

[7] Ryan Mac, Carolina Haskins, and Logan McDonald, *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, Buzzfeed News (February 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

claims."[8] Moreover, the Supreme Court has long recognized that "litigation is not [merely] a means of resolving private differences; it is also a form of political expression."[9] The fear that private companies will retaliate against those who dare to represent opposing interests not only deters the vindication of substantive rights, it threatens a key tool for social and political advocacy.

But the danger to free speech and public discourse is not limited to the realm of lawyers and litigation. Facial recognition can be used to punish and silence all sorts of critics: ongoing legal challenges by New York attorneys to MSG Entertainment's abusive use of facial recognition technology rely on a law that was passed to protect theater critics, but by analogy, it is not difficult to imagine that any one who speaks up against corporate interests may be targeted with facial recognition technology. In fact, there are reports that MSG Entertainment does maintain a blacklist of celebrities who have criticized its owner, James Dolan.[10]

The retaliatory use of facial recognition by private businesses to silence critics is antithetical to the values of free expression. But it also poses a danger to public health and safety and fair competition. Imagine a large restaurant chain that uses facial recognition to ban Yelp and Google reviewers with a history of commenting on health code violations or former employees that report labor violations. Such practices would allow businesses to evade public accountability for unlawful and insidious conduct, make it harder for consumers to protect themselves, deprive the market of the power to punish poor business practices, and impede the government's ability to identify businesses flouting industry regulations.

B. Business Owners Can Use Facial Recognition Technology to Engage in Unlawful Discrimination.

Profession may not be a protected class, but MSG's targeting of lawyers demonstrates that facial recognition technology can allow business owners to categorically exclude specific classes of people, including those protected by state and city anti-discrimination laws.[11] And because of the breadth of sources from which a facial recognition database can pull photos,[12] business owners may instead engage in proxy discrimination[13]—for instance, scanning patrons' faces and

[8] Letter from the Office of the New York Attorney General to Jamal Haughton, Executive Vice President General Counsel, Madison Square Garden Entertainment Corp. et al. (January 24, 2023), https://ag.ny.gov/sites/default/files/nys_oag_letter_to_madison_square_garden_entertainment_corp.pdf.

[9] NAACP v. Button, 371 U.S> 415, 429 (1963).

[10] Peter Botte, *James Dolan's Facial-Recognition Tech Also Targets Knicks Fans, Celebrities Who Criticize Him*, New York Post (December 29, 2022), https://nypost.com/2022/12/29/james-dolans-facial-recognition-tech-also-targets-knicks-critics/.

[11] N.Y. State Exec. Law § 296(2) ; New York City Human Rights Law § 8-107(4).

[12] *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, New York Times (January 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[13] *See* Anya Prince and Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 Iowa Law Review 1257 (2020),

comparing them to publicly available mugshots in order to ban individuals with a criminal history. While this policy is facially neutral in the sense that anyone could have a criminal history, longstanding disparities in policing means that it would disproportionately impact people of color.

Even where intent is absent, facial recognition can lead to discrimination. Numerous studies have revealed that face recognition software is plagued with bias, and specifically, that most face recognition algorithms perform less accurately on images of people of color, women, children, and the elderly, with Black women being subject to the highest rates of error.[14] Though there have been several high-profile, wrongful arrests of Black men,[15] misidentification by facial recognition technology is not limited to the policing context: in 2021, a Black teenager was barred from a roller-skating rink after a facial recognition system incorrectly matched her face to that of a patron who had previously gotten into a fight at the rink and subsequently been banned.[16]

Given such risk of both unreliability and racial bias, businesses should not even be permitted to use facial recognition technology for security purposes, as many business owners—including James Dolan—and policymakers have suggested is appropriate.[17] Beyond failing to mitigate

https://ilr.law.uiowa.edu/print/volume-105-issue-3/proxy-discrimination-in-the-age-of-artificial-intelligence-and-big-data.

[14] *See, e.g.*, Brendan F. Clare et al., *Face Recognition Performance: Role of Demographic Information*, IEEE Transactions on Information Forensics and Security (December 2012), https://docs.house.gov/meetings/GO/GO00/20190604/109578/HHRG-116-GO00-20190604-SD006.pdf; Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research (2018), https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, National Institute of Standards and Technology (December 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[15] *See* Kashmir Hill, *Wrongfully Accused by an Algorithm*, New York Times (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; Elisha Anderson, *Controversial Detroit Facial Recognition Got Him Arrested For a Crime He Didn't Commit*, Detroit Free Press (July 10, 2020), https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/; Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, New York Times (December 29, 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html; John Simerman, PSO Used Facial Recognition Technology to Arrest a Man. The Tech Was Wrong, The New Orleans Advocate (January 2, 2023), https://www.nola.com/news/crime_police/jpso-used-facial-recognition-to-arrest-a-man-it-was-wrong/article_0818361a-8886-11ed-8119-93b98ecccc8d.html.

[16] Randy Wimbley and David Komer, *Black Teen Kicked Out of Skating Rink After Facial Recognition Camera Misidentified Her*, Fox 2 Detroit (July 16, 2021), https://www.fox2detroit.com/news/teen-kicked-out-of-skating-rink-after-facial-recognition-camera-misidentified-her.

[17] Letter from New York State Senators to James L. Dolan (January 15, 2023), https://www.nysenate.gov/sites/default/files/article/attachment/electeds_letter_to_msg_1.15.23.docx

public safety threats, facial recognition systems that flag the wrong person nonetheless risk unnecessary police interactions that could lead not only to wrongful arrest, but to police violence—especially if the misidentified individual is a person of color or disabled.[18]

C. There are Insufficient Legal Safeguards to Expose, Prevent, and Redress the Harms Caused by Facial Recognition Technology.

The potential for New York City business owners to abuse facial recognition technology is especially concerning in light of the inapplicability of the few legal safeguards that do exist in the government context. First, the state and federal open record and freedom of information laws that have been crucial to uncovering the scope of harmful government surveillance in New York City—including the NYPD's relationship with facial Clearview AI, and its secret fund for surveillance tools[19]—can only reach private entities to the extent that they interact with public agencies and officials, and those interactions are documented in some form. So while New York City's law requiring commercial establishments that collect biometric information from customers to post a notice of that practice near all entrances[20] can shed some light on the singular question of which businesses may be utilizing facial recognition technology, the disclosure stops there, leaving New Yorkers with no knowledge of what type of biometric information is being collected, from whom, for what purpose, or by what type of technology, and therefore, with no opportunity to challenge the practice or seek redress from harm.

Second, federal and state constitutional rights to privacy, due process, and equal protection that might restrict certain government surveillance practices that constitute a search or seizure, that lack some form of legal oversight or formal procedure, or that disproportionately impact certain groups of people do not protect individuals harmed by such practices in the private sector. Of course, businesses are not entirely free from accountability: numerous local, state, and federal laws exist to prohibit discrimination and harassment and enforce health, safety, and fair business practice standards. But it is those very laws that are being undermined when companies like MSG Entertainment use surveillance tools to discourage legal representation and access to courts.

_.pdf/; Press Release, New York State Senate, Elected Officials & Privacy Advocates Demand MSG Entertainment End Use of Facial Recognition Technology on Fans (January 15, 2023), https://www.nysenate.gov/newsroom/articles/2023/brad-hoylman-sigal/elected-officials-privacy-advocates-demand-msg.

[18] *See, e.g.*, Mapping Police Violence, https://mappingpoliceviolence.org/; David M. Perry and Lawrence Carter-Long, *The Ruderman White Paper on Media Coverage of Law Enforcement Use of Force And Disability* (March 2016), https://rudermanfoundation.org/wp-content/uploads/2017/08/MediaStudy-PoliceDisability_final-final.pdf.

[19] Caroline Haskins, *The NYPD Has Misled The Public About Its Use Of Facial Recognition Tool Clearview AI*, Buzzfeed News (April 6, 2021), https://www.buzzfeednews.com/article/carolinehaskins1/nypd-has-misled-public-about-clearview-ai-use; Sidney Fussell, *The NYPD Had a Secret Fund for Surveillance Tools*, Wired (August 10, 2021), https://www.wired.com/story/nypd-secret-fund-surveillance-tools/.

[20] New York City Administrative Code § 22-1202.

What the incident at Madison Square Garden ultimately reveals is that a patchwork of laws directly or indirectly addressing some aspect of facial recognition and its attendant harms is insufficient for tackling the entire scope of the problem and will only lead to a game of whac-a-mole, with the technology perpetually outpacing the law. While a law that prohibits the wrongful refusal of admission to and ejection of ticket-holders from “places of public entertainment and amusement”[21] can protect criticism of or other adversarial action against those establishments, it cannot guarantee admission of those same critics from other venues like sports arenas, let alone non-ticketed places like restaurants or retail stores. And while the privacy and civil rights of students are recognized by a moratorium on the use of facial recognition technology in New York schools,[22] Amazon delivery drivers in New York forced to consent to facial recognition as a condition of employment,[23] on the other hand, are unprotected because no such moratorium has been passed in the employment context. And finally, legislative efforts that focus exclusively on government or police use of facial recognition[24] risk not only neglecting the retaliatory or discriminatory uses by businesses outlined above, but also leaving open a backdoor for law enforcement to access face recognition data in partnership with private businesses.

As more and more entertainment companies, retail stores, school systems, employers, and government agencies adopt facial recognition technology, and do so without public input or any form of democratic process, it is worth asking whether piecemeal oversight or legislation can adequately prevent the technology’s numerous risks posed to privacy, free speech and association, workers’ rights, and consumer protection.

We greatly appreciate the Committee’s attention to this critical issue, and thank you for the opportunity to submit this testimony.

[21] N.Y. Civil Rights Laws § 40-B. *See* Kashmir Hill, *Lawyers Barred by Madison Square Garden Found a Way Back In,* New York Times (January 16, 2023), https://www.nytimes.com/2023/01/16/technology/madison-square-garden-ban-lawyers.html.

[22] Assembly Bill A6787D, 2019-2020 Reg. Sess. (New York), https://www.nysenate.gov/legislation/bills/2019/a6787.

[23] Lauren Kaori Gurley, *Amazon Delivery Drivers Forced to Sign ‘Biometric Consent’ Form or Lose Job,* Vice (March 23, 2021), https://www.vice.com/en/article/dy8n3j/amazon-delivery-drivers-forced-to-sign-biometric-consent-form-or-lose-job.

[24] *See* Amnesty International, Ban the Scan New York, https://banthescan.amnesty.org/nyc/.

DAVIS, SAPERSTEIN & SALOMON P.C.

1-800-LAW2000

NEW JERSEY
375 Cedar Lane
Teaneck, NJ 07666
Phone: 201.907.5000
Fax: 201.692.0444

NEW YORK
39 BROADWAY, SUITE 520
New York, NY 10022
Phone: 212.608.1917

Testimony of Samuel L Davis, Esq before the NYC Council Committee on Consumer & Worker Protection February 24, 2022

"Oversight – The Use of Facial Recognition Technology in New York City Businesses."

Thank you Chair Velázquez and Council Member Bottcher for inviting me to speak today.

On November 27th, 2022, my associate Kelly Conlon was chaperoning her 9-year-old daughter's Girl Scout troop at the annual Christmas Spectacular Show at Radio City Music Hall.

Almost immediately after entering the building, she was confronted by two security guards. They handed her a one-page notice and then proceeded to eject her in front of her daughter and the other Girl Scouts.

Unbeknownst to her, Kelly had been flagged by a covert facial recognition system used by Madison Square Garden Group ("MSG").

What we have since learned, is that although MSG claims to use this technology at its properties to promote the safety and security of its patrons…That is simply not what is happening.

Sadly, it appears Ms. Conlon was identified by this technology because she was an employee of my firm and had therefore been put on a list that included lawyers from over 90 other firms. She was included on this list because my firm represented an individual in a personal injury case against a restaurant later acquired by MSG. A case Ms. Conlon did not have any involvement in.

MSG's use of facial recognition technology in this way has since led to significant public backlash as lawmakers, civil rights advocates, and the public recognize the serious dangers posed by MSG's use of a rapidly evolving surveillance tool.

Please do not let companies like MSG turn public accommodations into places where you leave your right to free speech at the door, where an opinion expressed in words on a T-shirt is your ticket to a lifetime ban, and where uttering, "sell the team" can get you excluded from venues all over the world.

When you weaponize facial recognition you invade our fundamental right to privacy. You stifle our freedom of speech and Americans, *and especially New Yorkers,* will not sit by and allow stadiums, theatres or restaurants in their city to be cleansed of dissident fans or customers who pose absolutely no threat to the safety of others.

In Kelly's words, she wants to take the humiliation she suffered and turn it into something positive.

She is grateful that the Council is taking a hard look at these dangerous and dystopian practices.

February 24, 2023

The Honorable Marjorie Velázquez
Chair
Committee on Consumer and Worker Protection
New York City Council
New York, NY

Written Testimony of SIA for Hearing on The Use of Facial Recognition Technology in New York City Businesses

Dear Chair Velázquez and Members of the Committee:

On behalf of Security Industry Association (SIA), a nonprofit trade association representing more than 70 companies headquartered in New York State and 1,300 nationwide, I appreciate the opportunity to participate in today's hearing. Our members provide a broad range of security and life safety products and services in the U.S and throughout New York. Among them are many developers of biometric technologies, including the leading providers of facial recognition software for a wide variety of government, commercial and consumer products.

We believe facial recognition – and all advanced technologies – must only be used for purposes that are lawful, ethical, and nondiscriminatory. When used effectively and responsibly, it can contribute to the safety of our communities and bring value to our everyday lives. It is always important that implementations of advanced technologies like facial recognition balance privacy concerns. SIA has published its *Principles for the Responsible and Effective Use of Facial Recognition* to provide guidance for public sector, law enforcement and private sector applications.[1]

I was asked to provide an overview of business use-cases for facial recognition. First, facial recognition technology is software that compares and matches facial images using mathematical means, to provide the functions of verification, identification, or similarity scoring. These three functions of facial recognition technology are in turn used in applications that are widely varied in purpose and configuration. For businesses, the purposes for using this technology generally fall into two categories that can be related: (1) enhancing business operations and (2) optimizing the functionality or security of products and services used by customers.

Declining costs and processing power required are driving adoption, as well as rapidly increasing speed and accuracy for the leading technologies, which are well above 99% in ongoing evaluations from the U.S. National Institute of Standards and Technology. Importantly, these advances have addressed "bias" issues present in some early technologies[2] developed prior to the introduction of modern techniques to build and configure algorithms. It is easier to use than other modalities, providing a touchless and even remote interface (for online account access as an example).

It is critical to understand that adoption of facial recognition technology by businesses is nearly always to augment or automate a pre-existing, underlying process of verification or identification that is already occurring through other, less effective means.

[1] https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/

[2] https://www.securityindustry.org/2021/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/

Commercial Uses

The security industry was an early adopter of biometric authentication, access control and security systems, to enhance the capabilities of these systems for customers in the commercial sector. However there are many business applications of the technology and related benefits:

- **Identity Verification to Prevent Identity Theft and Fraud:** Facial recognition provides an easily implemented biometric method for identity verification, as such tools increasingly serve as the backbone of the modern digital economy and allow consumers to safely utilize banking services and innovative new products and services online. Remote online identity verification serves many purposes, from account security to enhanced safety for gig economy workers and customers.

- **Contactless Payment and Access Credential:** Commercial use for payment and account access is growing, providing benefits like contactless payment, speeding lines and wait times, electronic venue tickets, and many other conveniences like VIP and reward system management.

- **Cybersecurity and Protecting Personal Data:** Like other biometric technologies (fingerprint, iris, etc.), facial recognition technology creates a numerical "template" from an individual's biological characteristics to compare with a template or templates already enrolled in a database or on a device. This numerical string of data is readable only within that software. Outside and apart from the software and database used to create it, this template by itself does not contain any personally identifiable information. Importantly, it cannot be used to re-create the digital image it was derived from. Each provider uses a different process to create and compare templates ("faceprints") unique to that particular proprietary software. A template created in one system cannot be used in another. In this way, the use of mathematical vectors acts as secure cryptography for facial recognition data, preventing identity hacking even if data is stolen, and naturally serves to limit unauthorized use by third parties. The collection, storage and processing of this data can easily be optimized to ensure privacy and security using encryption and other cybersecurity and privacy best practices applicable to other forms of personally identifiable information. Importantly, use of biometrics can help protect personal information by reducing or eliminating the sharing of biographical information (date of birth, Social Security Number, address, etc.), which is far more vulnerable to compromise and abuse during transactions.

- **Accessibility:** Some facial recognition applications can provide increased and customized accessibility for disabled persons. For example, they can assist people suffering from blindness, memory loss or prosopagnosia (face blindness) with recognizing friends and others.

- **Travel Facilitation:** Facial recognition is used by an increasing number of airlines to provide touchless curb-to-gate experience for air travelers. It is already used by the U.S. government to help travelers quickly clear customs returning to the U.S. at all airports, and many air, land and sea ports of entry, including cruise ports.

- **Gaming Industry:** Facial recognition is widely used by casinos for VIP recognition and enhanced customer service programs, voluntary problem gambler self-exclusion and enhanced security.

- **Health Care Industry:** Facial recognition provides touchless, authorized access to clean rooms and other restricted areas of hospitals. In assisted living facilities, it is leveraged to help protect vulnerable residents by screening visitors or providing staff with needed notifications regarding their status or location.

- **Sports and Entertainment Venues:** Facial recognition is being rapidly adopted by major U.S. venues to enhance fan experiences by enhancing mobile order pickup, age verification, streamlined payment and VIP area access. It is also being used to provide credentialing for secure locker room and field access.

- **Physical Access Control:** The technology provides a way for employees or other authorized individuals to securely verify their identity to access a secured space, to speed entry through security checkpoints, reduce touch points, and optimize building controls.

- **Facility Security Screening:** The technology gives security staff better information and context that allows them to make more informed decisions regarding individuals entering their facilities. Facial recognition technology can be used to cross-reference images with a limited gallery of known individuals created by the operator and provide alerts to staff for a wide range of purposes that protect occupants, such as controlling access in situations where there has threats of violence, or a protective order involving a specific individual has been issued. Many U.S colleges and K-12 schools are ensuring they have this capability to respond to growing threats of violence against staff and students.

- **Augmenting Loss Prevention Programs:** All major retailers have a loss prevention program that includes efforts to identify known organized retail crime (ORC) participants if they are on the premises. For years this has meant relying on the organization's case files and subject photos to screen individuals by visually comparing them against such lists, sometimes as simple as posting a shoplifter's photo to the entrance wall. If staff believe such an individual or group of individuals enter the premises, what happens next varies. Often greeting the individual and asking if they need any assistance is sufficient to communicate that they are being watched and can prompt the individual to leave if they have ill intentions. Facial recognition is increasingly used to augment these existing programs by anonymously comparing images of individuals entering a property against a (typically small) list and providing an alert to staff when where is a potential match. Some convenience stores and other smaller establishments are using the technology as a form of access control for similar purposes, where doors lock or unlock based on screening at the point of entry. The technology could also be used for post-event analysis of recordings from smash and grab incidents and "flash mob" theft.

Implementation Considerations

The extreme variation in facial recognition applications means that specific capabilities and implementation considerations such as privacy impact, are entirely dependent on the application-specific purpose, configuration, output and human role in the process that is being supported using the technology. End-users (versus technology providers) typically create and control access to this data, whether using on-premise, on-device or cloud-based solutions.

While many considerations can vary by application, SIA believes there are general principles that should guide all commercial and consumer application of facial recognition:

- **Legitimate Business Purpose**. Facial recognition technology should be used for legitimate, well-defined purposes relevant to the purpose of the organization, consistent with the rights of individuals.

- **Use Limitation**. Organizations should ensure access to a facial recognition system is limited to the minimum number of authorized individuals for authorized purposes**.**

- **Data Protection**. Facial recognition data should be obtained, used and stored only for legitimate business purposes, and linkage with PII should be minimized. Data should be protected according to information security and privacy best practices and any requirements in the organization's jurisdiction pertaining to the handling of

PII or other types of consumer data. Facial recognition data should be retained only for so long as needed for a legitimate business purpose, then destroyed.

- **Reasonable Notice**. Organizations should provide reasonable notice to individuals who, by continuing a course of action, will make their image subject to facial recognition analysis by the organization, unless public safety considerations make this infeasible**.**

- **Voluntary Applications Should be Consent-Based**. Enrollment in facial recognition applications that offer convenience or other commercial benefits should be based on prior consumer consent.

- **Clear Criteria for Safety/Security Applications**. Enrollment of an image in a facial recognition system for physical security, safety, fraud prevention or asset protection purposes should be guided by easy-to-understand written policies governing the criteria and human review process by which the enrollment is approved. Such implementations must also respect the reasonable expectations of privacy held by customers and individuals whose images or information are captured by security devices.

- **Provide Redress Mechanisms**. Organizations using facial recognition technology should provide a process for individuals to resolve any problems arising from their collected information. It may also require the ability to make a request for deletion/destruction of their facial recognition data.

Public Opinion

Awareness and public acceptance of facial recognition technology is growing. According to the most comprehensive public opinion research on the subject to date, a Schoen Cooperman Research survey commissioned by SIA, the vast majority of Americans are supportive of using facial recognition in everyday applications: 75% support use by airlines, 68% support use by banks for to secure access to accounts, 70% are comfortable with its use to improve security at their workplace. Overall, 68% of American adults surveyed it can make society safer.[3] See below a summary of these results.

SIA and its members strongly support the responsible use of advanced technologies, we stand ready to provide any additional information or expertise needed as you consider issues related to facial recognition technology.

Respectfully,

Jake Parker
Senior Director, Government Relations
Security Industry Association
Silver Spring, MD
jparker@securityindustry.org

[3] https://www.securityindustry.org/2020/10/07/extensive-new-poll-finds-most-americans-support-facial-recognition/.

SIA
SECURITY INDUSTRY ASSOCIATION

New Poll Shows Facial Recognition Technology Adding Value to Security and Convenience for Majority of Americans

OVERALL

→ **Nearly 6-in-10 Americans** are favorable towards facial recognition technology.

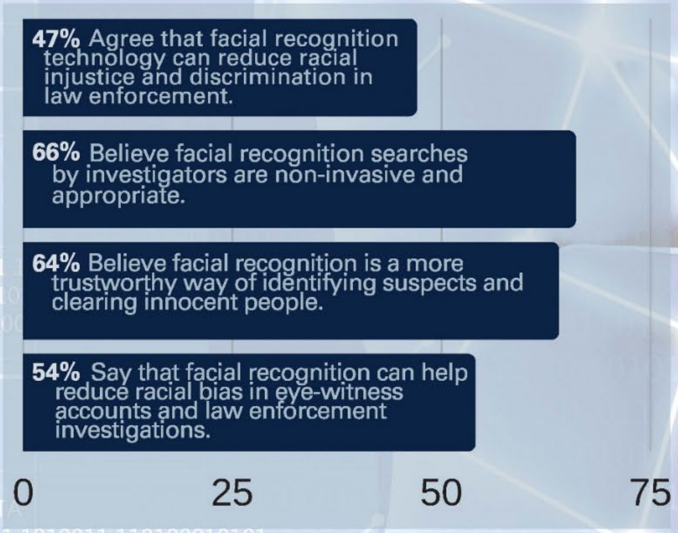
→ **7-in-10 Americans** believe facial recognition technology is accurate in identifying people of all races and ethnicities.

→ **Nearly 8-in-10 Americans** believe facial recognition technology can help find missing people.

USES OF FR

GROUP	IN FAVOR
Airlines	75%
Security at office buildings	70%
TSA or other airport security	69%
Banks	68%
Schools to screen adult visitors	67%
Police and law enforcement	66%

LAW ENFORCEMENT



47% Agree that facial recognition technology can reduce racial injustice and discrimination in law enforcement.

66% Believe facial recognition searches by investigators are non-invasive and appropriate.

64% Believe facial recognition is a more trustworthy way of identifying suspects and clearing innocent people.

54% Say that facial recognition can help reduce racial bias in eye-witness accounts and law enforcement investigations.

VIEW THE FULL SURVEY RESULTS AT

securityindustry.org

TRAVEL

78% **AGREE** Facial recognition technology can improve security systems.

74% **AGREE** Facial recognition technology can speed up security lines at airports and large events.

SCHOOLS

Americans support the use of facial recognition in schools, which can be used to alert school safety personnel if prohibited individuals and criminals, such as sex offenders, enter without permission

2/3 **OF ADULTS** Support schools using facial recognition technology to screen adult visitors

Say that these school safety benefits make them more supportive of facial recognition technology. **62%** **OF ADULTS**

Schoen Cooperman Research conducted 1,000 online interviews with a demographically representative sample of U.S. adults nationwide from August 5 to August 7, 2020. The margin of error is ±3% at the 95% level of confidence.

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT

40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (646) 602-5600

**STATEMENT OF
NINA LOSHKAJIAN
LEGAL FELLOW
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT ("S.T.O.P.")**

**BEFORE THE COMMITTEE ON CONSUMER AND WORKER PROTECTION,
NEW YORK CITY COUNCIL**

**FOR AN OVERSIGHT HEARING ON THE USE OF
FACIAL RECOGNITION TECHNOLOGY IN NEW YORK CITY BUSINESSES**

**PRESENTED
February 24, 2023**

Good morning, Chair Velázquez and members of the Committee on Consumer and Worker Protection. My name is Nina Loshkajian, and I am a Legal Fellow at the Surveillance Technology Oversight Project ("S.T.O.P."), a New York-based civil rights and anti-surveillance group. S.T.O.P. advocates and litigates against discriminatory surveillance. I appreciate the opportunity to testify today on the harms of facial recognition technology (FRT). We urge the Council to ban the use of this discriminatory and invasive software in places of public accommodation.

Thank you, Chair Velázquez, for organizing this important hearing. At the outset, though, we express disappointment at the fact that this hearing is focused on only one small aspect of FRT. The Council has seemingly ignored the growing threat from how this biased and dangerous tool is used by police and landlords. While we are heartened to see the Council paying attention to the issue of use in businesses, a much more comprehensive analysis of the unique harms of FRT in different contexts and legislation banning its use in multiple settings is necessary to protect New Yorkers now. It's been over a year since S.T.O.P. drafted legislation for the Council to ban the use of FRT, but the Council has not even introduced these bills yet or included them on any committee agenda.

When it comes to FRT in New York City businesses, New Yorkers should not be forced to accept biometric surveillance as part of simple activities like buying groceries or taking their kids to a baseball game. Yet this is the reality in our city, and it will continue to be until the Council acts. FRT puts New Yorkers, particularly Black and brown New Yorkers, at risk, and subjects them to discrimination.

I. Built-In Bias and Security Risks

FRT is biased and error-prone. Artificial intelligence ("A.I.") is the aggregation of countless human decisions, codified into algorithms. A.I. can learn to be just like us, exacerbating structural discrimination against marginalized communities.[1] In the case of facial recognition, this leads to systems that can be 99% accurate for middle-aged white men under ideal lighting in laboratory conditions, but can be wrong more than 1 in 3 times for some women of color, even under similar conditions.[2] The same exact software, the same exact hardware—but dramatically different outcomes for Black and brown New Yorkers. Numerous people, disproportionately Black, are wrongly arrested after being misidentified through facial recognition.[3]

Human bias infects A.I. systems. If a security camera learns who is "suspicious looking" using pictures of inmates, the A.I. replicates human bias and discrimination. When facial recognition software can only recognize two genders, we leave transgender and non-binary individuals susceptible to misidentification and wrongful arrest.[4] Immigrants suffer as well. A biometric scanning feature on a Customs and Border Protection (CBP) app failed to accept photos of dark-skinned African and Haitian migrants applying for asylum.[5]

[1] Sarah Myers West, Meredith Whittaker, Kate Crawford, *Discriminating Systems: Gender Race and Power in AI*, AI NOW INSTITUTE, p 6.

[2] Joy Buolamwini, Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceeds of Machine Learning Research*, vol 81, 1-15, 2018 p. 1.

[3] Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES, Dec. 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[4] Rachel Mentz, *AI Software Defines People as Male or Female. That's a Problem*, CNN BUSINESS, Nov. 21, 2019, https://www.cnn.com/2019/11/21/tech/ai-gender-recognition-problem/index.html.

[5] Melissa del Bosque, *Facial Recognition Bias Frustrates Black Asylum Applicants to US, Advocates Say*, THE GUARDIAN, Feb. 8, 2023, https://www.theguardian.com/us-news/2023/feb/08/us-immigration-cbp-one-app-facial-recognition-bias.

Further, allowing businesses to collect biometric information makes them an even more lucrative target for identity thieves and hackers.[6] Biometric identifiers are frequently used for ID verification and allocating public benefits; this makes an individual's biometric information an attractive target for fraudsters, as hackers can, and do use biometric identifiers to access computer systems.[7] More dangerous than other personal identifiers like a social security number, biometric identifiers are static and are almost impossible to change.[8] When a hacker acquires another person's biometric data, it puts them at risk for identity theft for the rest of their lives.[9]

II. Potential for Abuse

Facial recognition can identify any person, at any time, in any place—giving its operator incredible power. In recent months, James Dolan, the owner of Madison Square Garden Entertainment Corporation (MSG), has faced scrutiny for his use of FRT at the company's venues, including from New York State Senators[10] and Attorney General James.[11] Dolan has used the incredible power of FRT to seek vengeance against MSG's foes, blocking access to ticketholders who are affiliated with law firms involved in pending lawsuits against MSG. In one case, this meant ejecting a mother trying to watch the Rockettes show at Radio City Music Hall with her daughter's Girl Scout troop.[12] Business owners, especially wealthy, celebrity business owners, should not be allowed to use such dangerous tech to follow their whims or punish anyone who displeases them. It is easy to envision a situation in which a business uses FRT not only against perceived threats from outside the company, but also against its own employees who sue them for violating the law. The Council must act to stop retaliation against whistleblowers and others exercising their legal rights.

New York Police Department (NYPD) officers reported in open-records litigation that the department used FRT more than 22,000 times in just three years. Officers use pseudoscientific tactics that exacerbate the risk of error, such as running scans of celebrity lookalikes.[13] The Georgetown Law Center on Privacy and Technology documented the kinds of abuses that are "common practice" at NYPD.[14] One of the most egregious practices is that of routinely altering photos. The report revealed that NYPD edits of images "often go well beyond

[6] *US Government Hack Stole Fingerprints of 5.6 Million Federal Employees*, THE GUARDIAN, Sept. 23, 2015, https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints. Dan Rafter, *Biometrics and Biometric Data: What Is It and Is It Secure?*, NORTON, May 6, 2022, https://us.norton.com/blog/iot/what-is-biometrics.

[7] A. Dellinger, *Hackers Defeat Vein Authentication by Making a Fake Hand*, ENGADGET, Dec. 28, 2018, https://www.engadget.com/2018-12-28-hackers-defeat-vein-authentication-by-making-a-fake-hand.html.

[8] Anthony Ortega, *Do Biometrics Protect Your Data or Put Your Identity at Risk?*, SPICEWORKS, Oct. 8, 2018, https://www.spiceworks.com/it-security/data-security/articles/do-biometrics-protect-your-data-or-put-your-identity-at-risk/.

[9] *Is Your Identity at Risk from Biometric Data Collection?*, BeyondTrust (last accessed Oct. 6, 2022), https://www.beyondtrust.com/blog/entry/is-your-identity-at-risk-from-biometric-data-collection.

[10] Albany takes on attorney ban at Madison Square Garden (ny1.com)

[11] Andrea Vittorio, *Madison Square Garden Pressed by NY AG James Over Face Scans*, BLOOMBERG LAW, Jan. 25, 2023, https://news.bloomberglaw.com/privacy-and-data-security/madison-square-garden-pressed-by-ny-ag-james-over-face-scans.

[12] Sarah Wallace, *Face Recognition Tech Gets Girl Scout Mom Booted From Rockettes Show — Due to Where She Works*, NBC N.Y., Dec. 19, 2022, https://www.nbcnewyork.com/investigations/face-recognition-tech-gets-girl-scout-mom-booted-from-rockettes-show-due-to-her-employer/4004677/

[13] Khari Johnson, *NYPD Used Facial Recognition and Pics of Woody Harrelson to Arrest a Man*, VENTUREBEAT, May 16, 2019, https://venturebeat.com/2019/05/16/nypd-used-facial-recognition-and-pics-of-woody-harrelson-to-arrest-a-man.

[14] Clare Garvie, "Garbage In, Garbage Out: Face Recognition on Flawed Data," Georgetown Law Center on Privacy and Technology, May 16, 2019, https://www.flawedfacedata.com.

minor lighting adjustments and color correction," and in many instances "amount to fabricating completely new identity points not present in the original photo."[15]

Police also abuses FRT to surveil protestors. There are reports that the NYPD used FRT to target Derrick Ingram for his leadership of a peaceful Black Lives Matter protest. Police later surrounded Derrick's home with more than 50 officers as part of a retaliatory raid.[16]

Facial recognition searches are also skewed by where surveillance cameras are placed in our city. The technology is misused in a way that further replicates historical biased policing, with disproportionately high placement of cameras in low-income communities of color.[17]A recent analysis by Amnesty International found that "areas across all boroughs with higher incidents of stop-and-frisk are also areas with the greatest current exposure to facial recognition," and further, "the higher the proportion of non-white residents, the higher the concentration of facial recognition compatible CCTV cameras."[18]

III. Business Use of FRT in NYC and the Need for a Ban

Given the bias, invasiveness, and potential for abuse of FRT, it has no place in New York businesses. And yet it does. This year, the Mets implemented a facial recognition ticketing system at Citi Field.[19] In partnership with Wicket, a computer vision company, the Mets are encouraging fans to upload selfies on MLB.com to register their faces and then check-in at the gates. The Mets have touted this system as a new high-tech amenity. But FRT is not an amenity, it is discriminatory surveillance. And it is far from high-tech, as it often struggles to identify faces when people are wearing hats, seemingly an obvious issue for fans headed to a baseball game.[20] Additionally, many of the most popular venues in NYC, owned by MSG, now deploy FRT, and the technology is already used in some grocery stores.[21] Stores like Brooklyn Fare and Westside Market may be scanning the face of every single customer walking through their stores and storing that sensitive personal data indefinitely.

Public accommodations' use of FRT is already harming New Yorkers, and this use must be banned immediately. We have worked with Council Members to push for a suite of soon-to-be introduced legislation that would ban the use of FRT in three contexts: by law enforcement and other government agencies, by landlords, and by owners of places of public accommodation.

Our proposed legislation specifically prohibits places of public accommodation from using biometric surveillance tools and any information derived from biometric surveillance tools. Our bills also create a private right of action, empowering individuals whose biometric data has been collected illegally. This would prevent

[15] *Id.*

[16] 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.

[17] Eleni Manis et al., *Scan City: A Decade of NYPD Facial Recognition Abuse* (Surveillance Technology Oversight Project, July 8, 2018).

[18] *Inside the NYPD's Surveillance Machine*, AMNESTY INTERNATIONAL, https://banthescan.amnesty.org/decode.

[19] Andrew Cohen, *The New Face of Baseball: Mets to Roll Out Facial Recognition Ticketing at Citi Field*, SPORTS BUSINESS JOURNAL, April 1, 2022, https://www.sporttechie.com/the-new-face-of-baseball-mets-to-roll-out-facial-recognition-ticketing-at-citi-field.

[20] Sam Van Doran and David Siffert, *The Mets Should Steal Bases, Not Faces*, N.Y. DAILY NEWS, Sept. 15, 2022, https://www.nydailynews.com/opinion/ny-oped-bases-not-faces-mets-20220915-cuuul25ijnh5rbzbbsvmrbwauy-story.html.

[21] Lisa Fickenscher, *Retailers Busting Thieves with Facial-Recognition Tech Used by MSG's James Dolan*, N.Y. POST, Feb. 12, 2023, https://nypost.com/2023/02/12/retailers-busting-thieves-with-facial-recognition-tech-used-at-msg.

the types of abuses of the technology that we are seeing in places of public accommodation like MSG. We hope that this proposed legislation will be included on the agenda of a Council hearing in the near future, and that members of the Committee on Consumer and Worker Protection will support it, as urgent action is needed.

Thank you for the opportunity to testify today.

Testimony: Facial Recognition Technology for Businesses

2.24.23

NYC COUNCIL COMMITTEE ON CONSUMER AND WORKER PROTECTION

Tech:NYC is a nonprofit member-based organization representing over 800 technology companies in New York. Our membership includes hundreds of innovative startups as well as some of the largest tech companies in the world. We are committed to supporting New York's tech based economy and ensuring that all New Yorkers can benefit from innovation. Tech:NYC works with government and community partners to guarantee that New York remains the best place in the country to start and grow a technology company.

Facial recognition is a rapidly advancing technology that has only just begun to provide strategic uses in many aspects of daily life and business. As technologies that use cameras and are focused on security or crowd safety features continue to develop, facial recognition has the potential to help businesses in new ways -- many of which are still unforeseen. There are existing laws in place requiring public notification when this technology is used, and it is important for any businesses using it to do so with complete transparency and respect for personal privacy. Additionally, while the widespread and unchecked roll-out of this new technology may result in unforeseen circumstances, Tech:NYC also recommends for any new legal or regulatory limitations to be developed with responsible use cases in mind.

Facial recognition technology is often powered by artificial intelligence, which over time builds the product's recognition of known and unknown images, helping it to become more effective and accurate. Providing higher quality images ensures that the technology works more effectively and reduces the risk of misidentification. Facial recognition technology often acts as an initial notification, after which an individual is responsible for further review to confirm identifications. Artificial intelligence is currently at the forefront of innovation, and one of the most rapidly growing sectors within tech, which will continue to experience positive job growth in NYC in the years ahead. This is supported by Tech:NYC and Center for an Urban Future's 2022 Innovation Indicators report, which found that there are approximately 750 AI startup companies in NYC, up from 407 in 2016.

There are already many innovative products and services that use facial recognition technology, which are being used in homes and businesses across the country, and provide cost effective security solutions. Off-the-shelf home and business safety devices, like smart cameras, now have technology that can recognize faces, which help to track who is entering or requesting to enter a premise. This technology can also save previously seen faces, which helps to alert users of unknown visitors. Facial recognition can aid businesses which implement security measures, as well as those which have been targeted for crimes. It also is used for combating identity theft, which can be applied at high security businesses or those focused on securing intellectual property. Other security measures that can be enhanced by facial recognition are for providers of childcare or services for sensitive populations, where visitors can be confirmed by facial recognition technology. Businesses can also flag individuals with restraining orders or other legal prohibitions using this technology.

Facial recognition technology is often used by businesses and venues that have large numbers of customers or visitors. Facial recognition doesn't always need to identify actual individuals, as it can be used to count the number of visitors or patrons of large events or certain businesses as well. Its usage is often seen in the travel, sports and entertainment sectors, where the technology can provide more seamless access to venues and services. Banking is also a sector that is quickly implementing facial recognition tools, which will help to reduce fraud while modernizing ATM and mobile banking technology. While there are many creative and beneficial use cases for facial recognition software and products, it is crucial that there is full disclosure to the public on when it is used, and that patrons, customers and the public have a choice on when they can use it.

Tech:NYC recommends that businesses only use facial recognition technology for non-discriminatory purposes, and that the technology is always used in accordance with the law, which requires any NYC business using biometric identifying technologies to disclose its use via clear signage. There is much potential for this technology, and at the same time there is also potential for its abuse. Any abuse of this technology only detracts from the positive advancements that it can make to assist businesses and private citizens alike. Given the growing number of use cases and the positive trends in AI workforce, there is a significant local benefit for encouraging the development of this technology. Tech:NYC recommends that the City Council considers the positive impacts and use cases of this technology that will improve the safety and efficiency of local businesses when determining any new regulations or legislation to propose regarding facial recognition technology.

accessnow

Testimony of Willmary Escoto, U.S. Policy Analyst at Access Now, to the New York City Council Committee on Consumer and Worker Protection Regarding the Use of Facial Recognition Technology by New York City Businesses

1 March 2023

Dear Chair Velazquez and Members of the Committee,

Access Now appreciates the opportunity to submit testimony to the New York City Council regarding the use of facial recognition technology ("FRT") by New York City businesses. This submission concentrates on the harms of facial recognition technology and analyzes the status of important data protection regulations and legislation like Assembly Bill A1362 and how they can be strengthened.

Access Now is an international organization that defends and extends the digital rights of people and communities at risk worldwide. We have focused extensively on data protection and connectivity issues as an organization.[1] By combining innovative policy, user engagement, and direct technical support, we fight for a free and open internet that fosters human rights. We work directly with lawmakers at local, national, and international levels to ensure policy decisions are focused on the rights of people, particularly underrepresented populations.

We engage with fellow non-profit organizations and activist communities across civil society and campaign to ensure that new and emerging technologies and their investors, developers, and implementers "do no harm" first and foremost. This work includes also the Ban Biometric Surveillance campaign ("BanBS"), which calls for a prohibition on the uses of FRT and remote biometric recognition technologies that enable mass surveillance and discriminatory targeted surveillance. The "BanBS" letter has been signed by 193 civil society organizations from 63 countries worldwide.[2] Most recently, Access Now, Immigrant Defense Project, Just Futures Law, and over 35 human rights organizations sent a letter to Amazon Web Services calling on the company to end its agreement to host the United States Department of Homeland Security's (DHS) HART database.[3]

I. Ban applications incompatible with fundamental rights, such as biometric technologies that enable mass surveillance.

If New York truly wants to show leadership in promoting rights-respecting, trustworthy AI, it must ban the development and deployment of biometric technologies that enable mass surveillance in

[1] Access Now Privacy Archives https://www.accessnow.org/issue/privacy and Access Now Net Discrimination Archiveshttps://www.accessnow.org/issue/net-discrimination; Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[2] *Ban Biometric Surveillance Campaign Website*, Access Now, https://www.accessnow.org/ban-biometric-surveillance/.

[3] *Access Now Letter to Amazon Web Services concerning its hosting of the HART biometric* database (May 24, 2022), https://www.accessnow.org/cms/assets/uploads/2022/05/Letter-to-AWS-re-hosting-of-HART-biometric-database_24-May-2022_Final.pdf

publicly-accessible spaces. These technologies, by design, threaten people's rights and have already caused significant harm. The potential for abuse is too great, and the consequences too severe. No technical or legal safeguards could eliminate the threat they pose. Therefore, we believe they should never be used in public or publicly accessible spaces, either by governments or the private sector.

New York must make it an explicit policy objective to stop or ban applications of automated decision-making or AI systems in areas where mitigating any potential risk or violation is insufficient and no remedy or other safeguarding mechanism could fix the problem. Although some applications of facial recognition and remote biometric recognition claim to protect people's privacy by not linking to their legal identities, they can nevertheless be used to single out individuals in public spaces or to make inferences about their characteristics and behavior. In all such situations, it does not matter whether data are anonymized to protect personally identifiable information; the harm to our rights occurs because these tools are fundamentally designed for, and enable, the surveillance of people in a manner incompatible with our requests.

We have also seen a worrying development with private facial recognition providers compiling and amalgamating databases of "suspicious" individuals and sharing these databases with multiple clients. This, in effect, creates "nationwide databases" produced through warrantless private surveillance, shared between private companies. These are compiled at the discretion of untrained staff, are not subject to any oversight, and can lead to discrimination against individuals who appear on watchlists on all premises using such databases. Using these technologies to surveil people in city parks, schools, libraries, workplaces, transport hubs, sports stadiums, housing developments, and even online spaces such as social media platforms constitutes an existential threat to our human rights, and civil liberties must be stopped.

As you already know, facial recognition systems have accuracy issues, particularly for individuals of certain races, genders, or age groups. This can lead to false identifications, where authorities might mistakenly ban innocent people from events or locations. Additionally, these systems can infringe on individual privacy rights, as they capture and store biometric data without consent or knowledge from individuals.

Moreover, using facial recognition technology to target individuals based on where they work raises significant civil and human rights concerns. This practice can be viewed as discrimination or retaliation, as it penalizes individuals for exercising their legal rights to pursue litigation against a private entity. Such actions can create a chilling effect, preventing individuals from asserting their legal interests and human rights and limiting access to justice. Using facial recognition technology to identify and track individuals can also lead to stigmatization, social isolation, and harassment or persecution. As such, the Council must recognize the potential harm caused by private uses of facial recognition technology and mitigate these risks to protect individual rights and freedoms.

II. STRENGTHEN ASSEMBLY BILL A1362

While Assembly Bill A1362 is not perfect, it is an essential step toward combating the use of facial recognition by private entities. It provides a foundational step towards achieving a comprehensive data protection framework that would significantly alter the privacy landscape in New York. However, the Committee must continue to hear from civil society on this matter to ensure that the bill is the best it can be and reflects the needs of all New Yorkers. Below, I focus on essential provisions in Assembly Bill A1362 and recommendations to strengthen the bill.

Assembly Bill A1362 heightens protections for biometric data. Assembly Bill A1362 would also require covered entities to inform in writing and obtain written consent from individuals when collecting biometric data and additional consent to disclose it to third parties. Private entities must also establish a retention schedule and guidelines for permanently destroying biometric data. The bill also limits the data's monetization.

The collection and use of biometric data, particularly face data, poses significant risks to individuals.[4] Processing biometric data can lead to errors and present extreme privacy and civil rights risks. Data collection and processing can "reduce opportunities for Black, Hispanic, Indigenous, and other communities of color, or actively target them for discriminatory campaigns and deception."[5] Biometric surveillance is becoming an all-encompassing tool for companies to track where we are, what we are doing, and who we are with, regardless of whether we are suspected of a crime. For example, a mobile analytics company called Mobilewalla collected location data, device IDs, and browsing histories from more than 16,000 devices in Black Lives Matter protests in several major cities across the USA. With that data, Mobilewalla used "artificial intelligence" to predict people's demographics like race, age, gender, and zip code.[6] The protestors likely had no idea the company was collecting and processing data in such an intrusive way.

Companies are working hard to develop biometric and artificial intelligence systems based on biometric data, and they are doing it with essentially no safeguards.[7] Without reasonable limits, biometric technologies threaten to enable companies (and, by extension, law enforcement) to pervasively track people's movements and activities in public and private spaces and risk exposing people to forms of identity theft that are particularly hard to remedy. Assembly Bill A1362 places reasonable limits on biometric information retention, collection, and disclosure.

Assembly Bill A1362 ensures enforcement with a private right of action. Assembly Bill A1362 creates a private right of action, allowing aggrieved people to hold the violator directly accountable in state court. Data protection laws are only as effective as their enforcement, and allowing individuals to bring lawsuits will help ensure companies comply with the law.

Other private rights of action have been successful. For example, Illinois's biometric privacy law allows users whose biometric data is illegally collected or handled to sue the companies responsible.[8] The private right has been used to take action against Clearview AI for scraping the facial data of millions of people online.[9] It has also been used to take action against Facebook's practice of tagging people in

[4] Access Now and over 175 civil society organizations, activists, and researchers from across the globe are calling for a ban on uses of facial recognition and remote biometric recognition that enable mass and discriminatory targeted surveillance, https://www.accessnow.org/civil-society-ban-biometric-surveillance/.

[5] Eric Null, Isedua Oribhabor, and Willmary Escoto, *Data Minimization: Key to Protecting Privacy and Reducing Harm,* Access Now (May 2021), https://www.accessnow.org/cms/assets/uploads/2021/05/Data-Minimization-Report.pdf ; *see also* Cameron F. Kerry, *Federal privacy legislation should protect civil rights*, Brookings Institute (July 16, 2020), https://www.brookings.edu/blog/techtank/2020/07/16/federal-privacy-legislation-should-protect-civil-rights.

[6] C. Fisher, *Demographic report on protests shows how much info our phones give away*, Engadget (Jun. 25, 2020), https://www.engadget.com/mobilewalla-data-broker-demographics-protests-214841548.html; *see also* Caroline Haskins, *Almost 17,000 Protesters Had No Idea A Tech Company Was Tracing Their Location*, Buzzfeed News (June 25, 2020), https://www.buzzfeednews.com/article/carolinehaskins1/protests-tech-company-spying.

[7] For this and other reasons, the UN human rights chief recently called for a ban and moratorium on certain uses of AI. *Urgent Action Needed over Artificial Intelligence Risks to Human Rights*, United Nations (Sept. 15, 2021), https://news.un.org/en/story/2021/09/1099972.

[8] 740 Ill. Comp. Stat. Ann. 14/20, https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004.

[9] *Illinois Court Rejects Clearview's Attempt to Halt Lawsuit against Privacy-Destroying Surveillance*, ACLU-IL (Aug. 27, 2021), https://www.aclu-il.org/en/press-releases/illinois-court-rejects-clearviews-attempt-halt-lawsuit-against-privacy-destroying.

pictures with facial recognition software without consent.[10] Without a private right of action, individuals have to rely on federal or state enforcers, like the FTC, to protect their privacy. However, "[m]arginalized communities historically have not been able to rely upon the government to protect their interests, so individuals need to be able to vindicate their rights."[11] Thus, Assembly Bill A1362 should include a private right of action.

Assembly Bill A1362 could be improved. There are also several ways in which Assembly Bill A1362 could be improved. Here are just a few suggestions:

1. *Expand the scope of protected biometric information:* The current version of the bill only protects certain types of biometric information, such as facial recognition data, iris scans, voiceprints, and fingerprints. However, other types of biometric data could be collected by companies and used for identification purposes, such as gait recognition. The bill could be improved by expanding the scope of protected biometric information to include additional data types.
2. *Clarify the definitions used in the bill:* Some of the terms used in the bill, such as "biometric identifier" and "biometric information," are not clearly defined. This could lead to confusion about what types of data are covered by the bill. Clarifying these definitions could help to ensure that the bill is enforced consistently and effectively. "Processing" is also not defined or referenced in the bill.
3. *Strengthen the penalties for violations:* The bill's current version imposes fines on companies that violate its provisions. However, these fines may not deter companies from collecting and using biometric data without consent. Strengthening the penalties, such as by adding criminal sanctions or increasing the number of fines, could help ensure that companies take the protections the bill provides seriously.
4. *Provide more clarity around consent requirements*: The bill requires that companies obtain consent before collecting biometric data, but it does not provide clear guidance on what constitutes valid consent. Providing more clarity around the requirements for obtaining and documenting consent could help to ensure that individuals are fully informed about how their biometric data will be used and can make informed decisions about whether to provide it.

III. CONCLUSION

We encourage the Committee to use its *full* authority to protect persons against biometric systems and to hold a hearing on Assembly Bill A1362. We urge the Committee to regulate companies using these technologies in public spaces, publicly-accessible spaces, and places of public accommodation because such uses could enable mass or discriminatory targeted surveillance, including but not limited to their use in parks, schools, libraries, workplaces, transport hubs, sports stadiums, and housing developments.

Protecting biometric data is essential to ensure the privacy and security of all people in New York.
We urge the New York City Council to take action to ensure that our biometric data is protected to
the fullest extent possible. Thank you for your time and attention to these critical issues.

[10] Taylor Hatmaker, *Facebook Will Pay $650 Million to Settle Class Action Suit Centered on Illinois Privacy Law*, TechCrunch (Mar. 1, 2021), https://techcrunch.com/2021/03/01/facebook-illinois-class-action-bipa/.

[11] Letter to Roger Wicker *et al*., from Access Now *et al*. (Apr. 19, 2019), https://newamericadotorg.s3.amazonaws.com/documents/Letter_to_Congress_on_Civil_Rights_and_Privacy_4-19-19.pdf, at 3.

From: Jim S <jimsullivan20@gmail.com>
Sent: Monday, February 27, 2023 2:00 PM
To: Testimony
Subject: [EXTERNAL] NYC Council Committee on Consumer and Worker Protection Written Testimony 2/24/2023

James Sullivan written testimony to the New York City Council Committee on Consumer and Worker Protection
Friday, February 24th, 2023, via Zoom.

Thank you Madam Chair and members of the Committee. My name is Jim Sullivan, and I am SVP of Compliance and Chief Legal Officer for BIO-key International, a New Jersey-based provider of identity and access management solutions. We leverage biometrics in a positive way - we get rid of the scourge of passwords and stop hackers from being able to take over accounts. Put another way, we use biometrics - always with consent - to simplify how people get access to their workplace computers and applications by being able to recognize them, like a doorman. We also allow consumers to secure their digital identity to only them, so that others cannot take over their identity, even if they are a close family member who knows all their out-of-wallet ID verification questions. I have worked with biometrics and identity technologies and privacy for nearly twenty years. I am a member of the Georgia Bar Privacy & Technology Section, and was a contributing member of the Sedona Conference's Biometric Privacy Law Working Group, which aimed to help develop a model uniform template for biometric privacy law. I am a techie lawyer, with a Computer Science degree from Brown University. BIO-key is a member of the International Biometric Industry Association, an industry group of responsible biometric technology vendors. We don't develop surveillance or facial technology. We build fingerprint **authentication** technology, but we include facial recognition software from a third party vendor in our authentication products - with user consent - in order to secure access to computer systems.

What I want to convey in the context of this very charged topic are four points to expand on:

1. **Biometric Technology is Often Misunderstood and Subjected to Unwarranted Demonization.**
2. **Generalized NIST Reports Don't Reflect the Actual Products in Use.**

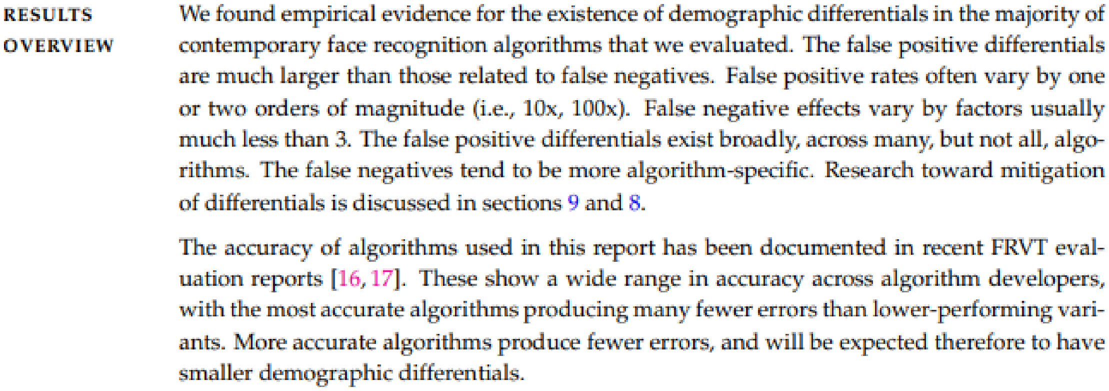
3. **Balance the interests of businesses operating in the city with individual privacy rights.**
4. **Narrowly Tailor Regulations to Prohibit the Misuse of Biometric Technology, not the Technology Itself.**

Expanding on these points:
I. **Biometric Technology is Often Misunderstood and Subjected to Unwarranted Demonization.**
Biometrics automates what people have done manually for centuries - recognize someone based on either a personal recollection of their features or using a trustworthy credential to compare such as a photo ID. It automates the centuries old "who goes there?" process that is fundamental to safety, security and informed decision-making.

A common concern arises relating to the implications of collecting biometric data. You heard well-intentioned critics today saying that biometrics can't be changed or reset, so if your biometric is compromised, the victim will be subject to "replay" attacks with the stolen data for life. This is understandable, but reflects a misunderstanding about how biometrics work. There are two parts to the flawed logical analysis. First, the fact that biometrics can't be "reset" is true - they are simply facts about the subject - their measurements. Critics point that out and then summarily but incorrectly conclude that biometrics represent the most dangerous, irrevocable PII. They then point out a second truth - that biometrics cannot be kept secret, because you are not a secret - you exist in public, always leaving fingerprints and your face available to observe. The contradiction in these statements - the "most dangerous PII" is based on something already exposed in public - points out the logical fallacy. If biometrics worked like passwords or private keys, relying on secrecy to function, then these truths - immutability and non-secrecy - would render biometrics useless. Thankfully **biometric systems do not rely on secrecy to be trustworthy**. Instead, they rely on **integrity or a chain of custody** to assure that a real person is being measured, the measurements protected against manipulation throughout the process of being securely compared with a securely-stored enrollment sample. If that process is carried out with integrity, then stolen biometric data is of no value as a means to impersonate someone. Said another way, just because someone knows what you look like, doesn't mean they can look like you. Properly implemented biometric systems ensure integrity of the entire process to prevent stolen data injection.

Humans make more mistakes doing so than facial recognition tools because they are subjective and in some cases have biases, and studies show that repetitive manual ID comparisons lead to comparison fatigue. When a biometric process is implemented with an **objectively unbiased algorithm**, then equitable outcomes are actually enhanced.

II. **Generalized NIST Reports Don't Reflect the Actual Products in Use.**
You heard today from Senator Holyman-Sigal and others that a 2019 NIST report indicated bias among the majority of algorithms tested. The speaker from SIA partially countered that claim. Characterizing an entire market by aggregating NIST results does not accurately reflect the marketplace of facial technology in use. The reason for this is that the NIST algorithm testing cited in the report Demographic Bias is free, and open to any and all commercial and non-commercial, competent and incompetent facial matching algorithms. A set of top-performing commercial algorithms that do not exhibit disparity in performance for any race sit among a sea of half-baked AI experiments, student research projects, and other baseline test efforts. The result is an eye-catching, but in truth misleading headline such as "A Federal report reveals that a majority of facial algorithms exhibit bias against people of color," despite the leading algorithms used by diligent commercial and government deployments never exhibiting any such bias defect. The report at issue even states that in the Results Overview: "These show a wide range of accuracy across algorithm developers, with the most accurate algorithms producing many fewer errors than lower-performing variants. More accurate algorithms produce fewer errors, and will be expected therefore to have smaller demographic differentials."



RESULTS OVERVIEW

We found empirical evidence for the existence of demographic differentials in the majority of contemporary face recognition algorithms that we evaluated. The false positive differentials are much larger than those related to false negatives. False positive rates often vary by one or two orders of magnitude (i.e., 10x, 100x). False negative effects vary by factors usually much less than 3. The false positive differentials exist broadly, across many, but not all, algorithms. The false negatives tend to be more algorithm-specific. Research toward mitigation of differentials is discussed in sections 9 and 8.

The accuracy of algorithms used in this report has been documented in recent FRVT evaluation reports [16, 17]. These show a wide range in accuracy across algorithm developers, with the most accurate algorithms producing many fewer errors than lower-performing variants. More accurate algorithms produce fewer errors, and will be expected therefore to have smaller demographic differentials.

III. **Balance the interests of businesses operating in the city with individual privacy rights.** Businesses make it easier for employees to do their jobs by eliminating passwords. Businesses are duty bound to maintain safe premises for their invitees, and want to know who they are allowing on their premises for liability reasons, and face constant threats of fraud. Businesses use biometric technology to efficiently meet those premises liability duties by recognizing individuals who have by their conduct created risk to other invitees of that business or to the business itself.

IV. **Narrowly Tailor Regulations to Prohibit the Misuse of Biometric Technology, not the Technology Itself.**

Prohibit the misuse and sale of data, not the use of the technology altogether. With consent or notice, a biometric technology can enhance consumer and business experiences in a positive way, getting past the process of proving who someone is and onto the process of helping them as a customer. If a biometric system demonstrates negligible or zero demographic differential in accuracy, then it can be a facilitator of equity rather than a detriment to it. Regulate the conduct that is improper, not the instrumentality. Good regulation will ensure that systems that could result in a negative interaction or detriment to consumers use algorithms that do not exhibit demographic differentiators.

Thank you for your consideration of my testimony, and I am available to answer any questions you may have.

Regards,

James "Jim" Sullivan
BIO-key SVP Strategy, Compliance and CLO

Emily Bach — New York City Council Hearing

My name is Emily Bach, and I'm a twenty-year-old student and activist, who spends her life working with survivors of sexual violence for a safer, more just world. I started this work when I was fifteen as a sophomore in high school. Normally, when people ask me how to get involved in organizing, I tell them about the field, but I also tell them about the risks. At almost every protest I've been to, there has been targetted, extreme surveillance. Sometimes this is through stingrays, which mine phone data, and other times, this is through facial recognition software, which we are here today to discuss. When we talk about surveillance, it is important that we center all of the ways it upholds a discriminatory, violent system of policing. Facial recognition software is anywhere from 35 to 100 times more likely to misidentify a Black woman than a white man. This only bolsters a system that incarcerates and punishes Black and brown people at significantly higher rates than white people, often for lesser crimes. But, it's also important that we discuss how facial recognition software not only upholds existing inequality, but prevents us from changing it. When I tell young people about how protestors tend to be aggressively, many of them tell choose not to get involved. These are people who want nothing more than to hold those that harmed them in the most intimate, personal way, accountable. These are people who want control over their own story, something that survivors of sexual violence are so often robbed on, and something that surveillance threatens. I say this not because anyone has anything to hide. Instead, I say this because the young people who want to build a better world aren't endlessly fearless. Many of us come to this work scared, scared of violence, scared of blowback, truthfully, scared of targetting. And this is precisely what surveillance does — in a world where protestors are aggressively surveilled, young people pursuing justice are targeted solely for believing a better world for each other. So, when we discuss facial recognition software, it's important that we clarify how it deters young people from pursuing what many of us would call justice. It's important that we clarify that these young people are overwhelmingly already marginalized — Black women, brown women, and trans people. Because surveillance systems aren't individual or discrete in the ways we're often led to believe. Facial recognition software in businesses relies on the facial recognition software used in our streets, in our public spaces, and around my college campus. In turn, facial recognition software in businesses would likely strengthen the cameras that I see each day as I walk to class and when I protest. I believe in a world where young people are encouraged to pursue justice, and I also believe that facial recognition software will not get us there. Instead, it will only heighten the barriers that young people, particularly marginalized young people, face when trying to build a safer world. These two things are connected, intimately, and it's important that our city responds accordingly.

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: 2/14/23

(PLEASE PRINT)

Name: Attiya Latif

Address: [redacted] Greene Ave [redacted]

I represent: Amnesty international USA

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:

(PLEASE PRINT)

Name: Nina Loshkajian

Address: [redacted] NY NY 10024

I represent: SURVEILLANCE TECHNOLOGY 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. ________ Res. No. ________

□ in favor □ in opposition

Date:

(PLEASE PRINT)

Name: JAKE PARKER

Address: 8455 Colesville Road Silver Spring MD. 20910

I represent: Security Industry Association

Address: 8455 Colesville Road Silver Spring MD 20910

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: ________

(PLEASE PRINT)

Name: Office of the Public Advocate

Address: ________

I represent: Jumaane Williams

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: ________

(PLEASE PRINT)

Name: Carlos Ortiz

Address: ________

I represent: DCWP - Assistant Commissioner

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: 2/24/23

(PLEASE PRINT)

Name: SAMUEL DAVIS

Address: 39 BROADWAY. N.Y. SUITE 520

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. ____________ Res. No. __________

□ in favor □ in opposition

Date: ______________

(PLEASE PRINT)

Name: Meg Foster

Address: [redacted] Saint Paul Street, [redacted]

I represent: The Center on Privacy & Technology at Georgetown Law

Address: 500 1st Ave NW Washington, DC 20001

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