Office of Technology & Innovation

OFFICE OF TECHNOLOGY AND INNOVATION TESTIMONY BEFORE THE NEW YORK CITY COUNCIL COMMITTEE ON TECHNOLOGY

Oversight - Facial Recognition Technology and the Collection of Biometric Data.

MARCH 2, 2026

Good morning, Chair De La Rosa, and members of the City Council Committee on Technology. My name is Alex Foard, and I am the Assistant Commissioner of Research and Collaboration in the Office of Technology and Innovation (OTI). Thank you for holding a hearing on this timely topic. I am pleased to have the opportunity to discuss my team's area of expertise with the Committee as it relates to today's oversight topic.

For those not familiar with our work, OTI's Research and Collaboration team leads the city's broad approach to artificial intelligence (AI) policy and governance. We have built a comprehensive portfolio from the ground up and will continue to expand it in this dynamically changing policy area.

The cornerstone of our work is the AI Action Plan, a first-of-its-kind framework to support responsible AI use in city government. Since its publication in October 2023, we have released two public-facing progress reports documenting its implementation. This plan supports agencies as they evaluate AI tools and associated risks to determine whether these technologies can help them deliver better outcomes for New Yorkers. I'm pleased to report that we have nearly completed all the actions described in the plan.

Most recently, we updated policies on "AI Principles & Definitions" and "Generative AI Preliminary Use Guidance," in response to technological advances in the field of AI. Additionally, we created new guidance on how city agencies should engage the public in discussing the use of AI for digital service delivery and have developed new instructional material for all city personnel to establish basic literacy on AI, focusing not just on Generative AI, but addressing the city's definition of AI more broadly. We continue to carry out research and planning related to AI risk management, focusing on elements such as an AI risk taxonomy, and a prototype risk assessment policy, risk review process, and risk monitoring process.

Another major responsibility of our team is leading agencies' compliance with Local Law 35. This law requires the disclosure of algorithmic tools that materially impact the rights, liberties, benefits, safety or interests of the public. A subset of an algorithmic tool is one that collects biometric identifiers (i.e.: facial recognition, fingerprints). In last year's report, three

agencies reported the use of tools collecting biometric identifiers. This year's annual Local Law 35 report will be released later this month. I am pleased to note that we have 100 percent participation from city agencies and will have a record number of algorithmic tools reported. This year marks the sixth cycle of compliance, and as we expand our guidance and offerings to municipal employees, we expect increased engagement from agencies in the future.

OTI is proud of our efforts to date to promote responsible use of AI tools in city government – and we will continue in the coming months to build on this strong foundation. Last year, we worked on a package of legislation with the Council – the GUARD Act – that requires the establishment of the Office of Algorithmic Accountability. This new office, which will be established by June, will undertake additional responsibilities that will expand on my team's work. These duties will include:

- Analyzing algorithmic tools submitted by agencies to determine whether there is risk that the proposed tool could result in discriminatory decision-making;
- Conducting and publicly reporting on pre-deployment assessments;
- Creating and maintaining a public-facing platform for submission of comments;
- Establishing a protocol with the Department of Investigation for receiving complaints from the public;
- Promulgating rules establishing basic compliance standards that all agencies must meet in developing, procuring, deploying, and using public-impacting artificial intelligence; and
- Expanding Local Law 35 reporting by publicly listing all artificial intelligence systems for which we have conducted a pre-deployment assessment.

We are also in the planning stage of implementing Local Law 25 of 2026, which requires us to conduct an AI Workforce Impact Study with the Department of Citywide Administrative Services (DCAS). This study will examine the impacts of algorithmic tools and automated employment decision tools on employees and the administration of their municipal duties.

OTI views AI technologies not as an aid to replace city jobs, but as a tool to support City employees' efforts to serve New Yorkers. Our objective is to prepare city personnel – whether they serve in technical roles or not – to effectively and responsibly work with and on AI. To that end, the AI Action Plan and its initiatives dedicated to building AI knowledge and skills within city government will serve as our north star.

As an update from the last hearing at which I appeared in June 2025, I wanted to share with the Chair that we are actively engaged with the Office of Labor Relations (OLR) on various efforts

my team leads. OLR is advising on the implementation of Local Law 25, has joined our AI Steering Committee, and has participated in our AI Speaker Series offered to city employees.

Thank you, once again, for the opportunity to testify today. I am happy to take Council Members' questions.

###

Testimony of Deputy Commissioner Samuel A.A. Levine
New York City Department of Consumer and Worker Protection

Before the Committee on Technology
Hearing on Introduction 213

March 2, 2026

Introduction

Good morning, Chair De La Rosa, and members of the Committee. My name is Samuel Levine, and I am the Commissioner of the Department of Consumer and Worker Protection (DCWP). Thank you for the opportunity to testify on Introduction 213.

Protecting New York's Workers

The NYC Department of Consumer and Worker Protection (DCWP) is the nation's leading municipal enforcement agency charged with delivering economic justice. DCWP leverages its authority to bring New Yorkers real economic relief and protect them from predatory, deceptive, and unfair practices that violate their rights as consumers and workers. This includes pioneering cutting-edge protections, such as the City's Consumer Protection Law, Protected Time Off Law, Fair Workweek Law, and Delivery Worker Laws, including the Minimum Pay Rate for delivery workers. Through licensing more than 45,000 businesses in over 45 industries, DCWP ensures fair competition and a level playing field for responsible small businesses that are integral to New York City's vibrant communities. DCWP also provides essential services such as free tax preparation and financial counseling to ensure New Yorkers keep more of what they earn and can plan for their futures. DCWP is committed to making sure New York City is a fairer, more affordable place to live.

Introduction 213

Turning to today's legislation, Introduction 213 would prohibit any place or provider of public accommodation from using biometric recognition technology to verify or identify a customer. It would also require customers to be notified if biometric identifier information is collected and would require written consent before any biometric recognition technology could be collected. Additionally, the bill would require any such information collected to be protected and for written policies regarding its use to be made available.

The use of biometric recognition technology is a burgeoning issue that affects New Yorkers. Local Law 3 of 2021 currently requires businesses that make use of biometric identifier information post a notice of such use at its entrances. DCWP provides on its website a template of the notice that must be used. This law is enforced through a private right of action, and while DCWP created the notice sign in 2021, the agency has no other authority related to this law. While we understand the concern surrounding biometric data, we do not have experience or expertise to speak to or regulate the use of this technology. As such, DCWP has no position on this legislation.

Conclusion

Thank you again for the opportunity to testify before the committee on today's bill. DCWP welcomes continued collaboration and partnership with all stakeholders and the Council to ensure that workplace protections and resources are available to all New Yorkers, regardless of immigration status.

Testimony of the

New York City Department of Housing Preservation and Development

to the New York City Committee on Technology on

Introduction 428-2026

March 2, 2026

Good morning, Chair De La Rosa and members of the New York City Council Committee on Technology. My name is Lucy Joffe, and I'm the Deputy Commissioner for Policy and Strategy at the New York City Department of Housing Preservation and Development.

Thank you for the opportunity to speak on Intro. 428, which would prohibit the use of biometric recognition technologies in residential buildings. As an agency, we care deeply about the intersection of tenants' rights and data privacy. With the proliferation of biometric technologies in public and residential spaces, there are real fears about the potential sharing of, misuse of, or unauthorized access to identifying information. The collection and use of this data raises potential privacy concerns for all New Yorkers, however, immigrant communities, survivors of domestic violence, and formerly justice-involved individuals, in particular, face heightened risks if sensitive data is improperly accessed or shared.

These privacy concerns are compounded by questions about the reliability of these technologies and the equity implications that follow. We understand that there is growing evidence that certain biometric technologies can be inaccurate, with documented disparities in performance across race, gender, age, and disability. Studies have shown that facial recognition systems, in particular, have higher error rates for women and people of color. In the housing context, inaccuracies are not a minor inconvenience; they could result in tenants being denied entry to their own homes or subjected to additional scrutiny. That risk raises serious equity and fairness concerns.

For these reasons, we support the goals of limiting the collection and use of sensitive identifying information in residential settings. We look forward to hearing more from the Council on how best we as a city can work collaboratively to address the concerns the bill seeks to address. Thank you, and I welcome your questions.

Comments on Oversight Hearing - Facial Recognition Technology and the Collection of Biometric Data.

Tech:NYC Comments — Last Updated: 3-2-26

Chair de la Rosa and Members of the Technology Committee,

Thank you for the opportunity to submit testimony as the Committee on Technology explores the critical intersection of biometric privacy and technological advancement. Tech:NYC represents more than 550 technology companies—ranging from early-stage startups to global leaders—all of whom share a commitment to fostering a digital ecosystem built on trust, safety, and responsible innovation.

The technology community recognizes that privacy and innovation are not mutually exclusive. In fact, thoughtful privacy protections are the bedrock of the public trust necessary for continued technological progress. As an organization that has spent years working toward a comprehensive data privacy framework at the State level, we appreciate the Council's engagement on these issues. However, as the Council considers Int. 213 and Int. 428, we urge a balanced approach that protects New Yorkers' biometric data without foreclosing the security and convenience benefits these technologies provide.

Refining Int. 213: Resolving Internal Inconsistencies

Tech:NYC supports the establishment of clear consumer rights and business responsibilities regarding biometric identifiers. However, to ensure a framework that provides clarity for businesses and predictable rights for consumers, the language of the law must be internally consistent.

We have identified a significant conflict within the current drafting of Int. 213:

- Subsection (a) establishes a framework for the collection and processing of biometric identifiers based on informed consent.
- Subsection (b), however, appears to create an outright prohibition on the use of biometric recognition technology.

These two provisions are in direct conflict. If a technology is prohibited entirely under subsection (b), the consent framework established in subsection (a) becomes moot. To resolve this and provide the "clear legal framework" necessary for responsible development, Tech:NYC recommends that subsection (b) be deleted. This would allow New York to align with emerging national models that favor robust, consent-based protections over total bans.

Int. 428: Balancing Security and Resident Access

Regarding Int. 428, which addresses biometric technology in multiple dwellings, Tech:NYC believes that security is paramount—especially when it concerns access to a person's residence.

While we agree that biometric data must be collected with strict consent and limitations on use, an outright ban ignores the practical safety benefits these tools offer New York families:

- Reliability: Residents, particularly children returning from school while parents are at work, often lose physical fobs or keys.
- Emergency Access: Biometrics provide a secondary, secure means of entry that a person "always has with them," ensuring they are never locked out of their own safe space.

Rather than a prohibition, Tech:NYC proposes that the law allow multi-tenant buildings to install this technology provided they have the express consent of the tenant. To that end, we suggest the following amendment to § 26-3008:

- "a. An owner of a multiple dwelling shall not install, activate, or use any biometric recognition technology that identifies tenants or the guest of a tenant **without the tenant or guest of the tenant that is being identified consenting to the collection and use of their biometric identifier information.**"
    - (Bold and underlined is new language)

New York has long been a global leader in both innovation and policy. By shifting from a framework of prohibition to one of informed consent and interoperability, the Council can ensure that New York remains at the forefront of the digital economy while protecting the fundamental privacy rights of its residents.

Effective governance begins with a strong foundation in data privacy. Tech:NYC and our member companies stand ready to work with the Council to advance thoughtful protections that reflect New York's values.

International Biometrics+Identity Association

1455 Pennsylvania Avenue, NW
Suite 400
Washington, DC 20004
www.ibia.org

ORAL TESTIMONY
Robert Tappan
Executive Director, International Biometrics + Identity Association (IBIA)
Re: Proposed Int. No. 213-A (0213-2026) & Int. No. 428 (0428-2026)

New York City Council, Committee of Technology
Monday, March 2, 2026; 10:00 am
City Council Offices - Eighth Floor, Hearing Room 2

Good Morning, Chair De La Rosa and Members of the City Council's Technology Committee. My name is Robert Tappan, and I am Executive Director of the International Biometrics + Identity Association. IBIA is based in Washington, DC, and I'm here today representing the biometrics and identity technologies industry on behalf of many of their customers and end-users who live and work here in New York City — small business owners, hotel operators, retail stores, apartment building owners, and residents — including seniors — who rely on biometric recognition technology every single day to protect their lives, their finances, their livelihoods and their property, as well as to protect those communities in New York City in which they live, shop, work, and serve.

We urge Council Members to oppose Proposed Int. No. 213-A **(0213-2026)** and Int. No. 428 **(0428-2026)**. Whether it's a corner bodega in the Bronx, a jewelry store in Queens, or a hotel or restaurant in Midtown Manhattan, facial recognition is not a luxury — it is a frontline defense against shoplifting, fraud, trespassing and violent crime. These businesses and establishments have been victimized repeatedly, often by repeat offenders who do so blatantly and brazenly.

Biometric and identity technologies allow owners to identify known bad actors before they strike again. Int. No. 213-A **(0213-2026)** would strip that protection entirely, banning identification technology at the very places most vulnerable to repeated theft and assault.

Int. No. 428 (0428-2026) poses an equally serious threat to the safety of New Yorkers at home. For seniors living alone in residential buildings or in assisted-care facilities, for families in neighborhoods with histories of break-ins and other crime, or neighborhoods with street corners that suffer from drug-dealing and gang activity, biometrics and identity technologies provide peace-of-mind, even when a key is lost or a fob is stolen. These systems reassure a tenant, store-owner or individual that the person who just walked through their lobby door is exactly who they say they are. Banning that technology doesn't make buildings safer or more secure — it makes them more vulnerable.

International Biometrics+Identity Association

We understand the Council's and citizens' concerns about privacy, and we take those concerns very seriously. But these bills do not regulate biometric technology — they attempt to eliminate it entirely. That is not a balanced or wise approach. It forces small business owners and property managers to choose between compliance with the law and the physical safety of their customers, employees, and tenants, along with the threat of property or inventory loss.

New York's small businesses are still recovering from the economic effects of the COVID pandemic and a very challenging economy. New York's residents, shoppers and store owners deserve to feel safe in their own buildings, residences, and places of business.

We urge, respectfully, that this Committee and the City Council as a whole reject these two proposals, and instead work with stakeholders on targeted regulations that protect privacy without leaving New Yorkers defenseless.

I would be pleased to answer any questions that you and your colleagues might have.

Thank you.

# # #

Robert Tappan
Executive Director

International Biometrics + Identity Association (IBIA)
1455 Pennsylvania Avenue, NW
Suite 400
Washington, DC 20004

Website: *www.ibia.org*
e-mail: *robert@ibia.org*

Testimony of

Segio De La Pava

Legal Director

New York County Defender Services

Before the

City Council Committee on Technology

Oversight - Facial Recognition Technology and the Collection of Biometric Data

March 2, 2025

Thank you, Chair De La Rosa, for holding this hearing to address the tidal expansion of facial recognition technology and the underexamined collection of biometric data. My name is Sergio De La Pava and I am the Legal Director of New York County Defender Services (NYCDS).

NYCDS is a public defense office that every year represents indigent New Yorkers in thousands of cases in Manhattan's Criminal Court, Supreme Court, and Family Courts. Since opening our doors in 1997, we have represented more than a half million clients in their criminal matters and witnessed firsthand the myriad ways the criminal legal system abuses and harms our clients.

Through this work, we see firsthand how large-scale surveillance decisions, made outside the courtroom and often by unelected private actors, then shape who is stopped, questioned, arrested, and ultimately prosecuted.

I. Background:

Over the past several years, biometric recognition technologies have increasingly been deployed in everyday spaces, including retail and food establishments, and residential buildings.[1] These

[1] Jay Stanley, *Retailers secretively using face recognition to spot "persons of interest" - Including for the Government*, ACLU (Jan. 20, 2026) at https://www.aclu.org/news/privacy-technology/retailers-secretively-using-face-recognition; Liam Quigley, *NYC Wegmans is storing biometric data on shoppers' eyes voices, and faces*, Gothamist (Jan. 3, 2026) at

systems collect and analyze uniquely identifying biological and behavioral characteristics, such as facial geometry, gait, voice patterns, etc. And unlike other forms of personal data, biometric identifiers, such as your face, cannot be changed or reissued if compromised, misused, or shared. That is why absent any regulation, once someone obtains your biometric information, they have it forever.

From our vantage point, we see how biometric surveillance implemented by private entities often has downstream consequences in the criminal punishment system. Information initially collected for purportedly non-law enforcement purposes is often later easily accessed by police, relied upon in investigations, or used to justify stops, questioning, and arrests. This typically occurs without notice to the individual, without meaningful opportunities to challenge the accuracy, and without the legal and procedural safeguards that must apply whenever the government itself conducts surveillance.

Nor are these deleterious impacts distributed evenly. Minorities, undocumented people, and the unhoused are far more likely to be subjected to biometric surveillance in the spaces they must access to meet their basic needs.[2] So, unsurprisingly, they are correspondingly more likely to bear the negative consequences of surveillance error and overreach.[3]

Vulnerable communities face increased risks of misidentification and persistent tracking by systems with well-documented bias and accuracy failures.[4] In 2019, the National Institute of Standards and Technology (NIST) published a report regarding the performance of 189 facial recognition algorithms, and found that many of them were between 10 and 100 times more likely to misidentify a Black or East Asian face than a white face.[5] Furthermore, for many of these algorithms, they were substantially less likely to correctly identify a Black woman than a member of any other demographic, with error rates being close to 35%.[6]

---

https://gothamist.com/news/nyc-wegmans-is-storing-biometric-data-on-shoppers-eyes-voices-and-faces; Amanda Benjamin, *5 things to know about surveillance in retail stores*, Legal Defense Fund (Jan. 16, 2026) at https://legaldefensefund.substack.com/p/5-things-to-know-about-surveillance; Erin Durkin, *New York tenants fight as landlords embrace facial recognition cameras*, The Guardian (May 20, 2019) at https://www.theguardian.com/cities/2019/may/29/new-york-facial-recognition-cameras-apartment-complex

[2] *Privacy & Racial Justice*, Electronic Privacy Information Center at https://epic.org/issues/democracy-free-speech/privacy-and-racial-justice/; Cynthia Griffith, *Homeless people surveilled at statistically higher rates*, InvisiblePEOPLE (Sept. 4, 2023) at https://invisiblepeople.tv/homeless-people-surveilled-at-statistically-higher-rates/; *Department of Homeland Security intensifies surveillance in immigration raids, sweeping in citizens*, PBS (Jan. 30, 2026) at https://www.pbs.org/newshour/politics/department-of-homeland-security-intensifies-surveillance-in-immigration-raids-sweeping-in-citizens.

[3] *Id*.

[4] *Biased technology: The automated discrimination of facial recognition*, ACLU Minnesota (Feb. 29, 2024) at https://www.aclu-mn.org/news/biased-technology-automated-discrimination-facial-recognition/,

[5] Beth Findley, *Why racial bias is prevalent in facial recognition technology,* JOLT Harvard (Nov. 3, 2025) at https://jolt.law.harvard.edu/digest/why-racial-bias-is-prevalent-in-facial-recognition-technology

[6] *Id. Biased technology: The automated discrimination of facial recognition*, ACLU Minnesota (Feb. 29, 2024) at https://www.aclu-mn.org/news/biased-technology-automated-discrimination-facial-recognition/.

Advocates for facial recognition technology will often point to inflated accuracy rates in a bid to support this intrusive technology. Critically, facial recognition technology is typically evaluated under controlled laboratory conditions that do not reflect real-world deployment. When tested in real-world conditions, such as airports and sports venues, performance drops significantly, with one study conducted by the NIST showing accuracy rates ranging from 36-87% depending on image quality and environmental factors.[7]

We can see these effects in the real world. In London, an independent review of their facial recognition technology showed that out of 42 matches, only 8 could be confirmed as absolutely accurate.[8] When these technologies are deployed in uncontrolled, real-world environments with constant movement, visual obstructions, and inconsistent image quality, they not only become less accurate overall but also exacerbate documented racial and gender disparities in misidentification.[9]

Even if facial recognition technologies were perfectly accurate, their deployment would still raise profound civil liberties concerns. The routine identification, tracking, and recording of individuals in public and in essential spaces undermines the fundamental right to privacy and erodes the expectation that people can move freely without constantly being surveilled. Accuracy does not cure the harms of surveillance; rather, it risks normalizing it. That is why the answer cannot be to amplify patterns of over-policing and surveillance that already cause great harm to these communities.

While the loss of privacy impacts everyone, the consequences are felt more acutely by communities that are already disproportionately policed and surveilled in their daily lives. Minority groups already face disproportionately high levels of policing, including higher traffic stops, searches, and use of force, compared to their white counterparts.[10] Widespread use of proven biased technologies will only further entrench these existing disparities.

Even in the absence of criminal charges, the collection and retention of biometric data can impose lasting collateral harm on a free society. The secret embedding of individuals into databases or watchlists is repugnant in itself. That this practice may then influence future police

---

[7] Center for Strategic and International Studies, *How accurate are facial recognition systems and why does it matter?* IMEdD (Oct. 27, 2020) https://lab.imedd.org/en/how-accurate-facial-recognition-systems/ citing Patrick Grother, et al., *Face in video evaluation (FIVE)* face recognition of non-cooperative subjects, National Institute of Standards and Technology (March 2017).
[8] Teo Canmetin, *Why we shouldn't trust facial recognition's glowing test scores*, TechPolicy Press (Aug. 18, 2025) at https://www.techpolicy.press/why-we-shouldnt-trust-facial-recognitions-glowing-test-scores/.
[9] *Id.*
[10] Nazgol Ghandnoosh, *One in five: Disparities in crime and policing*, The Sentencing Project (Nov. 2, 2023) at https://www.sentencingproject.org/reports/one-in-five-disparities-in-crime-and-policing/.

encounters or limit access to housing, services, and other critical aspects of public life is almost unthinkable but for the harsh guidance of recent human history.

So the importance of legislative action like these proposed bills is painfully apparent. Especially when considered alongside the New York Police Department's (NYPD) ever-growing and over-funded surveillance apparatus. The NYPD's budget remains near $6.4 billion, with huge swaths of it set aside for surveillance technology costs. This includes $94 million earmarked specifically for the Domain Awareness System.[11] This is the NYPD's centralized network of cameras, sensors, and data analytics that links to tens of thousands of CCTV feeds, license plate readers, and other monitoring tools across the city that input into a single searchable platform.

The astounding breadth of the NYPD's surveillance infrastructure has been aided and abetted along the way by insufficient oversight. A so-called free society cannot afford to repeat this error with the private sector. We must enact powerful protections that safeguard the once-powerful concept of human privacy. The secret collection of your biometric data, whether by the government or by a private actor, is so antithetical to this concept that it cannot be countenanced while pretending to value basic human dignity.

II. Proposed Legislation

A. Int. 0213-2026 (Hanif): In relation to prohibiting places or providers of public accommodation from using biometric recognition technology and protecting any biometric identifier information collected.

NYCDS supports this legislation. The proposed legislation addresses the growing use of biometric recognition technology in spaces that individuals must enter to meet basic needs, including grocery stores, pharmacies, and other public accommodations. These environments are particularly concerning because individuals, especially those with lesser resources, have little to no ability to avoid this surveillance without forgoing essential goods or services.

When combined with the high error rates and documented bias in these technologies, this practice poses disproportionate risk to communities that are already over-surveilled and over-policied. Racial minorities are disproportionately impacted by wrongful convictions, often due to mistaken or incorrect identification, and the further expansion of biometric technology into daily life threatens to amplify these harms.[12]

---

[11] *Inside the NYPD's surveillance machine*, Amnesty International at https://banthescan.amnesty.org/decode/index.html; *Automatic license plate readers*, NYCLU (July 23, 2025) at https://www.nyclu.org/report/automatic-license-plate-readers.

[12] Daniele Selby, *How racial bias contributes to wrongful conviction*, Innocence Project (July 17, 2021) at https://innocenceproject.org/news/how-racial-bias-contributes-to-wrongful-conviction/

To ensure the bill operates as intended, we recommend several clarifications. First, the prohibition of biometric recognition should be paired with explicit limits on disclosure of biometric identifier information to law enforcement absent judicial authorization. Second, the proposed legislation aims to prohibit the disclosure of biometric information in exchange for anything of value or profit with any third party. This section should be expanded to include a prohibition against sharing such information with government agencies unless there is judicial authorization. Third, the "deemed consent" provision under Admin. Code § 22-1204 (c), should be narrowly construed to avoid incentivizing businesses to design services that require biometric collection as a condition of access. Lastly, protections should apply to all individuals present in a public accommodation, not only those defined as "customers." This would prevent uneven application and gaps in coverage.

B. Int. 0428-2026 (Sanchez): Limiting the use of facial recognition technology in residential buildings.

NYCDS supports this legislation. The proposed legislation responds to the unique risks posed by biometric recognition technologies in residential settings. By prohibiting the use of biometric recognition technology to identify tenants or their guests, the proposed legislation recognizes that biometric surveillance in residential buildings raises distinct concerns because the surveilled cannot reasonably avoid or opt out of these systems. Limiting biometric identification in housing reduces the creation of records that can be later repurposed in ways residents or guests cannot anticipate or contest.

This particular concern is shaped by the City's past experience with police patrols in residential buildings under the "Clean Halls" or "Trespass Affidavit Program" (TAP).[13] Under this program, the NYPD patrolled residential buildings and almost indiscriminately arrested individuals, all under the guise of combating trespassers.[14] The practice resulted in a large number of stops and arrests of residents and their guests, predominantly Black and Brown individuals, without any individualized suspicion. Ultimately, it was all deemed to be unconstitutional.[15] But embedding biometric surveillance tools in residential buildings will recreate this discredited approach, and this time in permanent digital form. An impermissible enforcement model would be sneakily resuscitated into a far more powerful and uncontrollable beast. We cannot permit this.

---

[13] Ali Bauman, *An unconstitutional overreach? CBS2 investigates NYPD continuing banned practice of patrolling private buildings,* CBS News (May 18, 2023) at https://www.cbsnews.com/newyork/news/an-unconstitutional-overreach-cbs2-investigates-nypd-continuing-banned-practice-of-patrolling-private-buildings/

[14] *Id.*

[15] *Judge finds NYPD routinely makes unconstitutional street stops outside clean halls buildings across the Bronx,* NYCLY (Jan. 8, 2023) at https://www.nyclu.org/press-release/judge-finds-nypd-routinely-makes-unconstitutional-street-stops-outside-clean-halls

IV. Conclusion

We urge the Council to pass Int. 0213-2026 and Int. 0428-2026 to establish clear and enforceable limits on biometric surveillance. Absent these protections, there is a substantial risk that biased technologies will deepen discrimination and further entrench unequal surveillance practices.

If you have any questions about my testimony, please email policy@nycds.org.

Brooklyn Defenders

Brooklyn Defender Services
177 Livingston St, 7th Fl
Brooklyn, NY 11201

Tel (718) 254-0700
Fax (347) 457-5194
info@bds.org

TESTIMONY OF:

Talia Kamran, Staff Attorney

BROOKLYN DEFENDER SERVICES

Presented before

New York City Council Committee on Technology

Oversight Hearing on Facial Recognition Technology and the Collection of Biometric Data

March 2, 2026

My name is Talia Kamran and I am a Staff Attorney in the Seizure and Surveillance Defense Project at Brooklyn Defender Services. Brooklyn Defender Services (BDS) is a public defense office whose mission is to provide outstanding representation and advocacy free of cost to people facing loss of freedom, family separation and other serious legal harms by the government. I thank Chair De La Rosa for inviting us to testify today about the use of biometric identification technology in our city.

For 30 years, BDS has worked, in and out of court, to protect and uphold the rights of individuals and to change laws and systems that perpetuate injustice and inequality. After 29 years of serving Brooklyn, we expanded our criminal defense services to Queens. We represent close to 40,000 people each year who are accused of a crime, facing the removal of their children, or deportation. Our staff consists of attorneys, social workers, investigators, paralegals and administrative staff who are experts in their individual fields. BDS also provides a wide range of additional services for our clients, including civil legal advocacy, assistance with educational needs of our clients or their children, housing and benefits advocacy, as well as immigration advice and representation.

Many of the people that we serve live in heavily policed and highly surveilled communities. These predominantly low-income and Black and brown communities bear the brunt of our city's surveillance ecosystem, carrying a disparate proportion of surveillance load. Biometric identification technologies are deployed in public housing, on our public transit system, in our public benefits programs, and throughout our policing systems from the criminal legal and family policing systems and beyond.

BDS Supports the Regulation of Biometric Identification Technology Through Introductions 428 and 213

BDS supports both Introduction 428, which would limit the use of biometric identification technology in residential buildings, and Introduction 213, which would regulate biometric surveillance in places of public accommodation. These bills recognize the urgent reality that the use of biometric identification technology in daily life activities such as entering your home or

shopping for groceries are not neutral innovations that can be imposed on the public without regulation, transparency, and meaningful safeguards. Biometrics broadly encompass unique biological or behavioral characteristics such as facial features, fingerprints, voiceprints, iris patterns, or gait. They are immutable markers of personal physical identity that must be protected as intimately as any other personal information or property. Biometric identification technology refers to systems that attempt to identify or verify a person's identity by analyzing these unique characteristics using automated or algorithmic processes.

Biometric identification technology refers to systems that attempt to identify or verify a person's identity by analyzing these unique characteristics using automated or algorithmic processes. Biometric technology, like all artificial intelligence (AI) tools, must be trained on immense amounts of data. The more data they consume, the more powerful and invasive they become, until they erode individuals' privacy to such a great degree that there can no longer be a meaningful expectation of privacy whether you are buying medicine at a pharmacy or walking to the laundry room in your apartment building. As defenders, we have seen over the last several decades that the more the right to privacy is diminished, the fewer protections people have under the Fourth amendment, leading to a higher risk of legal system involvement, and wrongful convictions.

To Protect New Yorkers, City Council Must Pass Introductions 213 and 428

Introduction 213

The use of biometric identification technology in residential buildings raises serious constitutional and privacy concerns, particularly where access to one's home is conditioned on the surrender of one's biometric information.

These systems are frequently described as "virtual doorman" services and marketed as convenient and harmless. However, secure building access can be achieved through significantly less intrusive means, including key fobs, physical credentials, or regularly updated access codes. Unlike passwords or access cards, biometric identifiers—such as faceprints, palm prints, or voiceprints—cannot be changed if compromised. In the event that biometric data is leaked, there is no way to recover one's identity.

The collection and retention of biometric data in the residential context also implicates First Amendment protections. When landlords maintain access logs with biometric data, they can generate detailed records of tenants' associations, movements, and visitors. The existence of these databases creates risk not only of misuse by private actors, but also of access by government agencies. Immigration and Customs Enforcement's recent uptick in obtaining and purchasing data from private entities underscores the risk of allowing the unregulated

overcollection of personal data.[1] The agency has tracked individuals and circumvented legally required warrant practices with the express objective of facilitating deportation as well as targeting activists.[2]

The Constitution has long recognized the home as being entitled to the highest degree of protection from government interference. And yet, through biometric surveillance in residential apartment buildings, the safeguards afforded by the constitutions such as the warrant requirement for search become meaningless. For these reasons, BDS urges the Council to pass Int. 213.

Introduction 428

The risks to people's privacy and rights are placed at further risk by the use of biometric surveillance broadly in places of public accommodation. In addition to the erosion of individuals' privacy, the use of biometric surveillance in public venues places people of color at risk of discrimination and even false arrest.

Facial recognition technology is widely documented as racially biased and unreliable, particularly for people of color and women. In December 2023, the Federal Trade Commission banned Rite Aid from deploying facial recognition technology for five years after finding the company used flawed AI that falsely identified customers—disproportionately people of color and women—as shoplifters.[3] Acting on thousands of false matches, employees followed customers, searched them, publicly accused them, and in some cases contacted law enforcement.[3]

New York City does not need to wait for a finding of further harm before absorbing the lesson Rite Aid has to offer - the use of frequently inaccurate, highly invasive biometric identification technology does not enhance public safety; it amplifies bias and humiliation and harms consumers, particularly consumers of color.

In light of the serious threat to individuals' privacy, civil rights, and freedom, BDS strongly urges the City Council to pass Introductions 213 and 428.

---

[1] Joseph Cox, *CBP Tapped into the Online Advertising Ecosystem to Track Peoples' Movements*, 404 Media (Mar. 3, 2026), https://www.404media.co/cbp-tapped-into-the-online-advertising-ecosystem-to-track-peoples-movements/ (describing an internal DHS document showing that CBP purchased ad network-sourced location data to monitor phone movements, which can reveal residential locations without a warrant).

[2] NPR, *ICE Has Spun a Massive Surveillance Web. We Talked to People Caught in It*, (Mar. 4, 2026), https://www.npr.org/2026/03/04/nx-s1-5717031/ice-dhs-immigrants-surveillance-confrontation-deportation-mobile-fortify (reporting on ICE's use of Mobile Fortify and related facial recognition tools in law enforcement operations, including concerns that data aggregation and technology deployment bypass traditional warrant requirements).

[3] *FTC*, *Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology Without Reasonable Safeguards*, Federal Trade Commission (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without

The City Must Limit Its Own Agencies' Use of Surveillance Tools That Gather Intimate and Unnecessary Personal Data

While regulating the collection of biometric data in the private sector is urgently necessary, the legislation at issue today does not address the fact that *the biggest user of biometric identification technology in our city is our own city government.* New York City has spent billions over the last two decades building a vast surveillance infrastructure under the assertion that each new invasion of privacy will enhance public safety. Yet despite these investments, the promise of enhanced public safety has not materialized. Instead, what has expanded is the surveillance state in violation of New Yorkers' dignity, privacy, and Constitutional rights.

As public defenders, we see biometric recognition technology systems in daily use, impacting our clients in the criminal legal systems, the family separation systems, and the immigration systems. Underlying the spread of biometric identification systems is the national and global expansion of artificial intelligence generally. Computerized pattern matching engines are dominating the news and their dangers are being debated globally. We see AI surveillance tools deployed against our clients seeking unemployment benefits, facing evictions, or calling their loved ones from detention. The bills proposed here address one symptom of this proliferation but they do not ultimately address the underlying disease. To get to the core of this era-defining issue, it is critical to understand how machine learning or AI works. Fundamentally, to build an AI system, a developer needs a large amount of data to "teach" AI systems. Without those datasets, biometric identification technology would be impossible. AI, then, brings with it a voracious appetite for data. Thus, the conversation our community truly needs to have is not one centered around banning individual technologies but instead around defining rights to our data and, particularly, grappling with the inequities of the data surveillance economy we are already constructing.

Securus Voiceprint and Social Network Surveillance

Consider the example of Securus, the company contracted to provide phone call services for New Yorkers who are incarcerated in our city jails. Securus houses a database of every recorded jail call, in some cases even recording legally protected calls between individuals and their attorneys. Worse yet, Securus collects and stores voiceprints, capturing the unique vocal signatures of everyone who has ever placed or received a call from a New York City jail.

These voiceprints are not deleted when a person leaves custody, even if charges are dismissed or the person is found not guilty. Further, Securus's surveillance web is constructed without any court oversight and no need for a warrant. If a person is able to afford bail and avoid being held in city jails, law enforcement would only be able to eavesdrop on that person's calls with a specifically-issued warrant. Borrowed or gifted money would not be tracked. And voiceprints would remain that person's private information.

Under Securus's system, the mere reality of being poor and unable to afford bail means a New Yorker who is detained today, along with his or her entire community, has fewer rights, less privacy, and diminished dignity. More than 80% of those detained at Rikers Island are being held pretrial, which means they have not been convicted of anything, and are incarcerated due to an inability to afford bail. And the regime of data collection and surveillance turns on two axes of inequality–income and race. Significantly, more than 90% of individuals in pretrial detention are Black and brown people. Meaning that the data gathered by the Department of Corrections (DOC) through Securus - data shared with other agencies, used to train other AI-enabled surveillance tools - is almost exclusively gathered from low-income people of color.

The harm of the city's use of Securus extends past the fact that data is near-exclusively collected from low-income people of color. That data does not stay neatly within DOC control– Securus operates a platform known as "Threads," which aggregates and analyzes call metadata, voiceprints, billing names, addresses, and other identifying information across the thousands of correctional facilities nationwide that contract with the company. Through Threads, Securus pools data from facilities across jurisdictions and uses analytic tools to map social networks, identify shared contacts, track communication patterns over time, and generate association graphs. In effect, information from calls into or out of New York City jails is integrated into a nationwide database designed to reveal relational and behavioral patterns across institutions, threatening the privacy of anyone who contacts an incarcerated person. Threads interacts with other data platforms and has integration capabilities with Palantir, the surveillance and analytics corporation building interoperable databases to track immigrants, raising concerns that jail call data could be accessible to federal immigration authorities despite New York City's sanctuary laws.[4]

Engaging in the deeply human act of supporting someone in custody, something shown to reduce recidivism and improve outcomes, should not result in a person facing police surveillance. For these reasons, in order to protect New Yorker's digital identities and privacy, City Council must also pass Int. 96, the End Community Correctional Surveillance (ECCoS) Act, to ban the recording of jail phone calls and end the invasive and inappropriate surveillance of incarcerated people and their loved ones.

The NYPD Gang Database and Data-Driven Policing

The harm of biometric and other data collection through Securus does not exist in isolation. The skewed data collected through Securus calls is one of many used to build the modern surveillance infrastructure that threatens New Yorkers' Constitutional rights. Each invasive tool

[4] Gwynne Hogan, *ICE May Still Have Massive Access to Rikers Island Data Despite City's Sanctuary Status*, Documented (July 2, 2025), https://documentedny.com/2025/07/02/ice-may-still-have-massive-access-to-rikers-island-data-despite-citys-sanctuary-status/

feeds into other datastreams, like the NYPD's Domain Awareness System and requisite databases. As we have testified in our advocacy to abolish the NYPD's gang database, the NYPD's appetite for data to populate and justify its intelligence systems has led to coercive phone seizures, social media scraping, and the mass labeling of Black and Latine youth within the NYPD Criminal Group Database (widely known as the gang database) based on association rather than conduct.

The NYPD's gang database is part of the technological evolution of broken windows policing—transforming a regime of racially disproportionate street stops into one of racially disproportionate data collection, following the same trend of skewed collection present in the Securus context. Where officers once relied on physical stops and interrogations, they now use surveillance technology, secretive databases, and digital monitoring to track and criminalize Black and Latine youth. This shift does not make policing less discriminatory or less harmful; it simply makes it harder to challenge the basis for a stop or search in a criminal proceeding. Our courts are equipped to examine officer conduct and decisions regarding arrest and investigation as part of the constitutional guarantee that a person will only be arrested based on probable cause. However, when an officer relies on a database designation or algorithmic flag to justify a stop, search, or arrest, the database itself cannot be subjected to the same adversarial scrutiny, if its use is even introduced in court at all.

The gang database extends and deepens the NYPD's long-standing patterns of racialized policing, embedding them into data systems that follow young people indefinitely, regardless of whether they have ever committed a crime.

The injustice of the database ranges from the harm of racial discrimination to severe due process harms. Once a person is designated as a gang member by the NYPD, they have no means to challenge that label in court or elsewhere. This "gang" designation often results in higher bail amounts, increased pre-trial incarceration, and the inability to access much needed programming. Even if a person's charges are dismissed or they complete a sentence, their name remains in the database, leaving them vulnerable to continued police scrutiny and abuse. Unlike unlawful stops and searches, which can sometimes be challenged in court, gang designations offer no pathway for removal, making them a tool of unchecked policing with no oversight.

The transition from widespread stop-and-frisk to expansive data policing has not reduced racial disparities; it has only made them more insidious. The people we represent experience persistent police scrutiny, unjustified stops, and coercive interrogations simply because they live in heavily policed communities. The gang database also causes Black and Latine immigrants to be more susceptible to immigration detention and deportation based on little more than where they live and who they are friends with; this risk of separation from their families and communities is

particularly acute after the recent designation of certain gangs as terrorist organizations.[5] Moreover, young asylum seekers who are fleeing violence from gangs in their home countries are often themselves erroneously labeled as gang members.[6] Given how inaccurate and biased the database is and the risk to people's safety and rights it poses its existence presents an unjustifiable risk of harm.

We do not need this database, and we have ample documentation that it is inaccurate, discriminatory, and easily abused. The NYPD has demonstrated a willingness to bend or break rules to access and share information, and there is no credible way to regulate a system built on such deeply flawed foundations. We call on the City Council to pass Int. 96 to abolish the highly discriminatory and harmful NYPD gang database.

New York Needs Comprehensive Data Protection Legislation, Not Piecemeal Defense Against Data Collection

Taken together, Securus, the gang database, and the rapid expansion of private facial recognition systems demonstrate that AI-powered surveillance tools impose social and institutional costs that should cause us to seriously rethink their rapid acquisition and use in the private and public sector. The predictive or matching capacity of any AI system depends entirely on the dataset on which it is trained and the inputs it continuously ingests. When those datasets are drawn from systems already shaped by racialized policing, economic inequality, and selective enforcement, they help create surveillance and predictive policing tools that are built from distorted baselines.

In this way, historically skewed data becomes the foundation for future suspicion, creating a feedback loop in which past discrimination is encoded as algorithmic bias. The result is not simply flawed technology, but an infrastructure that both depends upon and intensifies the erosion of privacy and equality. These tools require the continuous extraction of personal data in order to exist, and in doing so they transform human bias into automated decision-making power, embedding inequality deeper into the institutions that govern liberty. For these reasons City Council must seriously consider the harm in unchecked data collection–biometric and otherwise–by the NYPD, DOC, and other government entities as urgently as it addresses the private sector.

New York City has the opportunity to end the game of data privacy whack-a-mole in a more holistic way by passing comprehensive data protection legislation that recognizes personal data as precious personal property, that cannot be bought or sold without our informed consent, or accessed by our government, outside of the bounds of the Constitution. There is no way to build a humane surveillance state. There is, however, a way to build a city grounded in dignity,

[5] Terrorist Designations of International Cartels - United States Department of State, https://www.state.gov/terrorist-designations-of-international-cartels/.
[6] See Jonanthan Blitzer, "How Gang Victims Are Labeled As Gang Suspects," The New Yorker, January 23, 2018, https://www.newyorker.com/news/news-desk/how-gang-victims-are-labelled-as-gang-suspects.

constitutional protections, and racial justice. Passing these bills, while committing to broader data justice reforms, is an essential step toward that future.

We thank the Committee on Technology for your commitment to addressing these issues. If you have any questions, please do not hesitate to contact Jackie Gosdigian, Supervising Policy Counsel, at jgosdigan@bds.org.

Testimony by Director of Research and Policy Cynthia Conti-Cook of the Collaborative Research Center for Resilience

To the Committee on Technology of the New York City Council Chair Carmen de la Rosa

On March 2, 2026 Regarding Why New York Communities Need Limitations on the Growth of Biometric Collection and Recognition Technologies

Submitted Written Testimony on March 4, 2026

The Collaborative Research Center for Resilience (CRCR) is focused on ensuring that government use of technology to access public goods, such as municipal identity or education, do not undermine democracy. We investigate and conduct community-centered action research to support key interested and affected groups who are often left in the dark (e.g., workers, impacted community members, elected officials). We do so with the intention to elevate meaningful participation in governance across areas with profound impact on our daily lives.

We testify in general support of both Introductions 428 and 213 limiting biometric recognition technology. However, we also urge the Council to expand such limitations to ban biometric collection technology in addition to recognition technology. We also encourage all reporting and use limitations to apply equally to all agencies, including police. We urge the Council to consider not just the direct harms of surveillance policing but to thoroughly also explore the foreseeable community harms, as described in further detail below. This includes the potential for taxpayers to pay three times for the harms created by new technologies: for the harm; to compensate for the harm; and for the vendors' overpriced harmful service.

In addition to the harms to individuals and communities that result from surveillance policing, we must also look ahead to the harms of surveillance pricing. While the biometric industry claims that safety and security is their mission, biometric collection infrastructure is the foundation required for surveillance pricing. Surveillance (or euphemistically "dynamic") pricing is when the cost of goods changes based on the customer profile of each person who walks in. It predicts what they might buy again, for example if it is an allergy-safe product or favorite brand that the customer has a pattern of buying. The prices are then set according to the real-time prediction for that customer. Perhaps on a hot summer day, for example, someone who is lactose intolerant may pay a premium price for an allergy-safe ice cream.[1]

Surveillance pricing relies on identification technology infrastructure—and biometric collection and recognition technologies are a key component. Identity technologies include digital drivers licenses, passports, digital wallets, and age verification technologies. The future capacity to integrate biometrics and other identity technologies with other information gathering technologies powered by AI is exactly the type of future use case industry associations brag about in front of government buyers—surveillance pricing but for police. Instead of changing a price, a police tool might have a dynamic "risk" score that lets them "click and frisk" to see more details about who that person is, where they work, and what kind of basis an officer might have to engage them.[2] Therefore the community harms we must consider are not just present day uses of biometrics for security but for identity technology infrastructure as a whole. Where else can we have this conversation when so many of these decisions are being made in budgets and pilot projects with little public oversight or reporting?

---

[1] Press Release, UFCW, UFCW Launches National Campaign to Ban Surveillance Pricing on Groceries (Feb. 12, 2026), https://www.ufcw.org/press-releases/ban-surveillance-pricing-on-groceries/; Jay Stanley, *"Surveillance Pricing" Hurts Consumers, Incentivizes More Corporate Spying on Them*, ACLU (Sep. 12, 2025), https://www.aclu.org/news/privacy-technology/surveillance-pricing.

[2] See The Net, https://thecrcr.org/wp-content/uploads/MovieNight-the-Net-V20.pdf

Community harms also include what we collectively lose—control over our creativity and cohesion. The enhanced capacity of corporations to extract fragments of our content, to collect our biological information from us–from our recordings, images, voices, and text–and create something they then sell back to us (or worse, blackmail us with) also foreseeably harms us all. Granting these systems access to our biometrics empowers AI bots with an even richer set of tools with which to continue plundering our identities, our creativity, and our community. Look what they did to the entirety of information we've already granted them access to over the past few decades of social media — why would we believe our biometrics will be more carefully treated than any other content that has been exploited when shared?

The AI-bot-ification of social media has made it impossible to know who is real and who is an avatar—the ingredients of each avatar being disassembled pieces of ourselves. While agentic AI is wreaking havoc on social media platforms, snatching identifying information, and blackmailing us with deep fakes, we must at the very least have a moratorium on all government procurement of biometric collection and recognition technology, a comprehensive assessment of the potential harms incoming through identity technology infrastructure in the commercial and government sectors, place more expansive limitations on insurance policies that pressure businesses to install biometric technologies and restrain biometric data collection.

There are so many ways that businesses are accessing data through sales but also through mergers and acquisitions–the prohibitions on sale of biometric data must also understand the various forms of investment, corporate maneuvering, and market capture that technology companies engage in to seize control of data assets. Public sector data is a hot commodity because it holds the keys to creating tools that governments might buy. Long-term sole-source government contracts guarantee years of predictable work and leverage over future contracts. This political economy of the technology sector cornering government marketplaces must be analyzed alongside complex forms of public procurement that also impact what companies can access sensitive personal identifying information, including biometrics, by virtue of being a public sector vendor (or parent company).

It is this level of concern we ask the City Council to consider here. We look forward to working together to understand the implications of this digital public infrastructure and protect our democracy and communities.

Collection of Biometric Data Increases Surveillance of New Yorkers

Biometric recognition and collection technology, deployed in tandem with other surveillance technology like artificial intelligence (AI), enables corporations and the government to easily track and control the behavior of Americans as they shop at the grocery store, post on social media, and other ordinary, daily real life and digital activities. The previous mayoral administration, for example, proposed using digital wallets to modify eating behavior of benefits recipients.[3]

[3] Nicholas Liu, *How the Adams Administration is Thinking About Blockchain and Cryptocurrency*, Gotham Gazette (Mar. 17, 2023), https://www.gothamgazette.com/city/11883-city-council-mayor-adams-blockchain-cryptocurrency/

The proliferation of AI happening at the same time as the scaling of biometric identity technologies by small businesses and landlords should cause caution given the well publicized problems associated with their deployment, including false matches leading to wrongful arrests[4] or unjust exclusion from businesses,[5] the lack of reliability in its ability to accurately identify people of color,[6] and its dubious compliance with constitutionally protected rights such as due process.[7] Despite the uptick in the usage of these invasive technologies, Congress has not passed any legislation regulating these types of invasive technologies.[8] Some states and cities have attempted to fill this regulation gap by passing moratoriums or bans on the use of facial recognition technology by police because of the foreseeable harms it introduces to communities.[9]

Law enforcement agencies use this technology to surveil and target immigrants,[10] protesters,[11] public housing residents,[12] legal observers,[13] and the broader community at large. However, limiting the usage of this technology only for police does not protect communities from the harms associated with surveillance

---

[4] Crystal Cranmore, *Man's Wrongful Arrest Puts NYPD's Use of Facial Recognition Tech Under Scrutiny*, ABC 7 (Aug. 27, 2025), https://abc7ny.com/post/man-falsely-jailed-nypds-facial-recognition-surveillance-tech-failed/17664671/; *Woman Wrongly Accused of Carjacking Loses Lawsuit Against Detroit Police Who Used Facial Technology*, CBS NEWS (Sep. 4, 2025), https://www.cbsnews.com/detroit/news/woman-wrongly-accused-carjacking-loses-lawsuit-detroit-police-used-facial-tech/.

[5] Jay Stanley, *Retailers Secretively Using Face Recognition to Spot "Persons of Interest" — Including For the Government*, ACLU (Jan. 20, 2026), https://www.aclu.org/news/privacy-technology/retailers-secretively-using-face-recognition.

[6] U.S. COMMISSION ON CIVIL RIGHTS, THE CIVIL RIGHTS IMPLICATIONS OF THE FEDERAL USE OF FACIAL RECOGNITION TECHNOLOGY 3 (Sep. 2024), https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf.

[7] *Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology*, NEW AMERICA, June 3, 2021, https://www.newamerica.org/oti/briefs/civil-rights-concerns-regarding-law-enforcement-use-of-face-recognition-technology/?utm_source=chatgpt.com.

[8] Amy B. Cyphert, *Confronting the Challenges of Regulating Artificial Intelligence*, 20 FIU L. REV. 82, 85 (2025), https://ecollections.law.fiu.edu/cgi/viewcontent.cgi?article=1741&context=lawreview; Bobby Allyn, *With No Federal Facial Recognition Law, States Rush to Fill Void*, NPR (Aug. 28, 2025), https://www.npr.org/2025/08/28/nx-s1-5519756/biometrics-facial-recognition-laws-privacy.

[9] Jake Laperruque, *Status of State Laws on Facial Recognition Surveillance: Continued Progress and Smart Innovations*, TECH POLICY PRESS (Jan. 6, 2025), https://www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations/.

[10] Jude Joffe-Block, *Immigration Agents Have New Technology to Identify and Track People*, NPR (Nov. 8, 2025), https://www.npr.org/2025/11/08/nx-s1-5585691/ice-facial-recognition-immigration-tracking-spyware.

[11] Sheera Frenkel & Aaron Krolik, *How ICE Already Knows Who Minneapolis Protestors Are*, NY TIMES (Jan. 30, 2026), https://www.nytimes.com/2026/01/30/technology/tech-ice-facial-recognition-palantir.html.

[12] Zachary Groz, *Five Unanswered Questions About Eric Adams's Expanded Surveillance at NYC Public Housing*, NEW YORK FOCUS (Aug. 12, 2025), https://nysfocus.com/2025/08/12/unanswered-questions-adams-surveillance-big-apple-connect.

[13] Alfred Ng, *DHS Accused of Using Surveillance Tech to Track Legal Observers in Maine*, POLITICO (Feb. 23, 2026), https://www.politico.com/news/2026/02/23/dhs-accused-of-using-surveillance-tech-to-track-legal-observers-in-maine-00792722.

technology. For example, corporations like Wegmans[14] and Madison Square Garden[15] employ this technology on New Yorkers as they grocery shop and attend concerts.

If corporations are permitted to collect this kind of sensitive data, law enforcement agencies can issue demands to gain access, undermining local bans on the use of facial recognition technology by police.[16] It is widely reported that the Department of Homeland Security (DHS) has done just that—purchasing personal data collected by private companies, circumventing the Fourth Amendment's requirement to get a warrant before searching private information.[17] Thus, the collection of biometric data of consumers by private corporations expands the government's ability to surveil and micro-target vulnerable communities.

Corporations can also use this data themselves to target certain consumers for higher prices[18] and wrongfully refuse admission to their businesses.[19] Given the federal government's embrace and expanded use of these technologies,[20] it is imperative that local governments like New York City step in to protect city communities from foreseeable harm and large scale liability.

---

[14] Tim McNicholas, *Some Wegmans Locations, Including 1 in NYC, are Now Using Facial Recognition Software on Customers. Here's Why.*, CBS NEWS (Jan. 5, 2026), https://www.cbsnews.com/newyork/news/wegmans-facial-recognition-software-new-york-city/.

[15] Kashmir Hill & Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, NY TIMES (Dec. 22, 2022), https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html.

[16] Paige Oamek & Andrew Giambrone, *Not Just Wegmans: More NYC Retailers Using Facial Recognition as Tech Outpaces Law*, GOTHAMIST (Jan. 12, 2026), https://gothamist.com/news/not-just-wegmans-more-nyc-retailers-using-facial-recognition-as-tech-outpaces-law; Sheera Frenkel, *Lawmakers Ask Tech Companies What User Data They Provided to D.H.S.*, NY TIMES (Feb. 25, 2026), https://www.nytimes.com/2026/02/25/technology/lawmakers-tech-companies-dhs.html.

[17] Anika Venkatesh & Lauren Yu, *DHS is Circumventing Constitution by Buying Data It Would Normally Need a Warrant to Access*, ACLU (Jan. 12, 2026), https://www.aclu.org/news/privacy-technology/dhs-is-circumventing-constitution-by-buying-data-it-would-normally-need-a-warrant-to-access.

[18] FTC, FTC SURVEILLANCE PRICING 6(B) STUDY: RESEARCH SUMMARIES: A STAFF PERSPECTIVE 1, 5 (Jan. 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf .

[19] Kashmir Hill & Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, NY TIMES (Dec. 22, 2022), https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html; Press Release, Federal Trade Commission, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without.

[20] *See, e.g.,* Anthony Kimery, *Trump Administration Expands Facial Recognition While Erasing Oversight Policy*, BIOMETRICUPDATE.COM (Oct. 31, 2025), https://www.biometricupdate.com/202510/trump-administration-expands-facial-recognition-while-erasing-oversight-policy?utm_source=chatgpt.com; Matt O'Brien, et. al., *Hegseth Warns Anthropic to Let the Military Use the Company's AI Tech As it Sees Fit, AP Sources Say*, AP (Feb. 24, 2026), https://apnews.com/article/anthropic-hegseth-ai-pentagon-military-3d86c9296fe953ec0591fcde6a613aba.

Biometric Collection Aids Surveillance Pricing Which Harms Consumers

The collection of consumer data and advancements in AI technology allow companies to target particular customers and charge them higher prices, a practice called surveillance pricing.[21] For example, grocery stores who engage in surveillance pricing collect information on consumers to build individualized profiles through various means including data collected from in-store kiosks with interactive touchscreens, virtual storefronts like apps and websites, and location data from IP addresses.[22]

Stores also collect biometric data on consumers while shopping in-store.[23] Grocery stores are increasingly using electronic shelf labels which enable them to change prices at any time.[24] These digital price tags, combined with the information collected through surveillance pricing tactics, increase the risk that stores will monitor and track shoppers as they move throughout a store, changing prices based on the information they are collecting and storing.[25]

This also puts retail workers at risk as grocery store clerks would be the ones bearing the brunt of angry customers who notice they are being charged more than other shoppers for the same item.[26] Although General Business Law 349-a, the first surveillance pricing law enacted in the country, went into effect last year, it only requires businesses to disclose when their prices are set by algorithms that use the consumer's personal data, not prohibit the actual practice of surveillance pricing.[27]

As many New Yorkers struggle to make ends meets, companies should not be permitted to surveil the shopping habits of their customers in order to charge unfair prices. The collection of biometric data on consumers when they visit stores gives companies more tools to set individualized prices and expand surveillance pricing systems.

---

[21] FTC, FTC SURVEILLANCE PRICING 6(B) STUDY: RESEARCH SUMMARIES: A STAFF PERSPECTIVE 1, 5 (Jan. 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf .

[22] *Id.* at 8–9.

[23] Liam Quigley, *NYC Wegmans Is Storing Biometric Data on Shoppers' Eyes, Voices and Faces*, GOTHAMIST (Jan. 3, 2026), https://gothamist.com/news/nyc-wegmans-is-storing-biometric-data-on-shoppers-eyes-voices-and-faces.

[24] Press Release, UFCW, UFCW Launches National Campaign to Ban Surveillance Pricing on Groceries (Feb. 12, 2026), https://www.ufcw.org/press-releases/ban-surveillance-pricing-on-groceries/; Jay Stanley, *"Surveillance Pricing" Hurts Consumers, Incentivizes More Corporate Spying on Them*, ACLU (Sep. 12, 2025), https://www.aclu.org/news/privacy-technology/surveillance-pricing.

[25] *See* Press Release, UFCW, UFCW Launches National Campaign to Ban Surveillance Pricing on Groceries (Feb. 12, 2026), https://www.ufcw.org/press-releases/ban-surveillance-pricing-on-groceries/.

[26] *Id.*

[27] Press Release, Kathy Hochul, Governor, New York, Protecting New Yorkers From Secret Online Price Hikes: Governor Hochul Announces Nation-leading Surveillance Pricing Law Now in Effect (Nov. 24, 2025), https://www.governor.ny.gov/news/protecting-new-yorkers-secret-online-price-hikes-governor-hochul-announces-nation-leading.

Private Biometric Collection Facilitates More Surveillance by Law Enforcement

Companies who build surveillance tools and collect data on Americans regularly sell this information to law enforcement. For example, Clearview AI built a biometric database from images of people it collected on the internet and social media profiles without permission from the websites or individuals in the photos.[28]

Its AI system created "faceprints" of each person and allows users to search for matches when a "probe photo" runs against its database, identifying the matching faceprint and giving a link to the websites where the matching photo originated.[29] Clearview sold its technology, which can be utilized without a search warrant or probable cause, to law enforcement clients and Immigration and Customs Enforcement (ICE).[30] Law enforcement have used this technology to target immigrants, activists, and protesters, circumventing privacy and due process requirements.[31]

Clearview also sold its technology to corporations like Macy's who allegedly used Clearview on its customers.[32] When stores are permitted to collect biometric data with their security cameras, there is an increased risk that companies like Clearview could purchase access to these feeds and give this information to their law enforcement clients. This exacerbates the climate of fear for immigrants who are concerned that a trip to a grocery store like Wegmans could lead to their biometric data getting into the hands of ICE.[33] Recently, investors in Home Depot raised concerns that the company is sharing the biometric data it collects of its customers while they shop with ICE, as the agency has conducted many raids in its store parking lots, emphasizing the danger that allowing private actors to collect biometric data can open up our communities to increased policing and displacement.[34]

Collection of Biometric Data Accelerates Development of Harmful Agentic AI Systems

AI companies are now developing and employing agentic AI tools–and access to biometric identifying data is a key component to how they plan to operate. Unlike generative AI, which uses data sets to create text, images, and video, agentic AI systems are semi or fully autonomous, making decisions and performing tasks with little to no human input or supervision.[35] As more companies develop this kind of technology,

---

[28] Luke O'Brien, *The Shocking Far-Right Agenda Behind the Facial Recognition Tech Used by ICE and the FBI*, MOTHER JONES (May & June 2025), https://www.motherjones.com/politics/2025/04/clearview-ai-immigration-ice-fbi-surveillance-facial-recognition-hoan-ton-that-hal-lambert-trump//

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] Liam Quigley, *NYC Wegmans Is Storing Biometric Data on Shoppers' Eyes, Voices and Faces*, GOTHAMIST (Jan. 3, 2026), https://gothamist.com/news/nyc-wegmans-is-storing-biometric-data-on-shoppers-eyes-voices-and-faces.

[34] Arriana McLymore & Ross Kerber, *Amid ICE Raids, Some Home Depot Investors Want to Know How Law Enforcement Uses its Surveillance Data*, REUTERS (Jan. 16, 2026), https://www.reuters.com/sustainability/boards-policy-regulation/amid-ice-raids-some-home-depot-investors-want-know-how-law-enforcement-uses-its-2026-01-16/.

[35] Beth Stackpole, *Agentic AI, Explained*, IDEAS MADE TO MATTER (Feb. 18, 2026), https://mitsloan.mit.edu/ideas-

their desire to collect more biometric data will grow as biometric data enables the agents to operate more efficiently.[36] Government regulation is needed to counteract this push for more data collection as the harms of agentic AI are already materializing.

For example, banks use AI agents to decide whether to approve or deny a consumer's application for a mortgage.[37] These AI agents rely on information outside traditional sources like credit reporting agencies.[38] They also base their decisions on data collected from an individual's "digital footprint" to determine an applicant's creditworthiness, much of it collected without the user's awareness.[39] AI agents also rely on historical data to make lending decisions which replicate patterns of systemic discrimination and bias, harming Black and Latino applicants.[40]

The rapid development of agentic AI also poses a real threat to displace entry-level jobs.[41] Regulators have struggled to reel in abuses of these kinds of technologies, allowing proliferation with limited guardrails and supervision.[42] As companies integrate biometric ID collection into these systems, the risk that our biology and identities will become vulnerable to the chaos and unpredictability of agentic AI will grow.

Similarly, people exploit these vulnerabilities by snatching our loved one's likenesses and manufacturing a crisis we respond to out of fear and without thinking. Rather than regulating and preventing the proliferation of chaotic AI and create responsibility within technology companies to prevent AI bots from plundering our information, the biometric industry irresponsibly urges us to upload even more sensitive data to our digital twins.

Lawmakers, trying to catch up when they do attempt to regulate, tend to focus on the current usages of these technologies and miss the trends on how these technologies are developing and the potential future harms associated with evolving technology. For example, AI agents are already reinforcing discriminatory practices and threatening the livelihoods of many Americans with or without access to our biometric data. If we allow companies to collect the biometric data of their customers, we permit them to use this data in

---

made-to-matter/agentic-ai-explained.

[36] Mohamed Lazzouni, *The Role of Biometric Identity in the Age of Agentic AI*, FORBES (Nov. 21, 2025), https://www.forbes.com/councils/forbestechcouncil/2025/11/21/the-role-of-biometric-identity-in-the-age-of-agentic-ai/.

[37] Korin Munsterman, *When Algorithms Judge Your Credit: Understanding AI Bias in Lending Decisions*, 17 UNT DALLAS ACCESSIBLE L. (2025), https://www.accessiblelaw.untdallas.edu/post/when-algorithms-judge-your-credit-understanding-ai-bias-in-lending-decisions.

[38] *Id.*

[39] *Id.*

[40] *Id.*; Will Douglas Heaven, *Bias Isn't the Only Problem with Credit Scores – And No, AI Can't Help*, MIT TECHNOLOGY REVIEW (June 17, 2021), https://www.technologyreview.com/2021/06/17/1026519/racial-bias-noisy-data-credit-scores-mortgage-loans-fairness-machine-learning/.

[41] Ezra Klein, *How Fast Will A.I. Agents Rip Through the Economy?*, NY TIMES (Feb. 24, 2026), https://www.nytimes.com/2026/02/24/opinion/ezra-klein-podcast-jack-clark.html.

[42] Tom Wheeler, *The Three Challenges of AI Regulation*, BROOKINGS (June 15, 2023), https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/.

conjunction with other unregulated technologies like digital drivers' licenses and digital wallets, making us even more vulnerable to the harms associated with them. It is critical that the City considers these technologies as interconnected systems, not technologies used in isolation, to ensure that the regulation sufficiently captures both current uses and future developments in the deployment of surveillance technology.

The City Council Must Address the Real Harms of Surveillance Technology

Given the extensive harms inherent in the use of biometric collection and recognition technologies, it is critical that the Council take action to protect New Yorkers. We support the Council's desire to combat biometric recognition technology in places of public accommodation, but we also encourage the adoption of stronger measures that directly address communities' core concerns around privacy and surveillance by prohibiting data collection in addition to limiting how data is used.

We urge the Council to approach surveillance technology with the goal of *preventing* the collection of New Yorkers' personal data, rather than solely regulating how their data is being used. While regulations on the use of personal data are valuable, they are also limited in how much protection they provide. The collection and storage of personal data, regardless of intended purpose, creates significant risks to privacy and security. Personal data is always vulnerable to data breaches or leaks once harvested—a danger heightened by the uniqueness of biometric data.[43] Additionally, the very real economic value of such data provides powerful incentives for corporations to sell data even when such sales are illegal. This incentive is further strengthened by the difficulty of tracking illicit disclosures, the existence of loopholes that allow the sale of aggregated or supposedly "anonymized" data,[44] and weak financial penalties that pale in comparison to the profits offered by the data-mining industry. Even if companies are unwilling to take the risk of directly selling data, other legal workarounds threaten the security of personal data, such as transfers through corporate mergers and acquisitions.[45]

In the Netherlands, for example, a legislative task force is considering blocking a merger between a Dutch identity technology vendor that operates its national ID system and an American company. The concerned

---

[43] Report of the New York City Council Committee on Consumer Affairs and Business Licensing on Int. 1170-2018, (Dec. 10, 2020), https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3704369&GUID=070402C0-43F0-47AE-AA6E-DEF06CDF702A&Options=Advanced&Search [accessible as a PDF by clicking hyperlink "Committee Report 12/10/20"]

[44] Public Interest Advocacy Centre, *Consumers Anonymous? The Privacy Risks of De-Identified and Aggregated Consumer Data*, (Oct. 6, 2011), https://www.piac.ca/wp-content/uploads/2014/11/piac_consumers_anonymous_paper_final_6oct2011.pdf (explaining methods of re-identification from aggregated or de-identified data)

[45] Daniel Ilan, *Privacy in M&A Transactions: Personal Data Transfer and Post Closing Liabilities*, HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE, (Nov. 10, 2016), https://corpgov.law.harvard.edu/2016/11/10/privacy-in-ma-transactions-personal-data-transfer-and-post-closing-liabilities/ (discussing liabilities involving personal data during the mergers and acquisitions process).

members of the legislature wonder whether the merger is a national security threat by virtue of how much power the vendor holding the entirety of the Dutch civic infrastructure has.[46]

Beyond the technical challenges of regulating how personal data is handled, an approach to surveillance that only regulates corporations *after* they collect people's data misses the core problem of surveillance: *people do not want to be the source of information when it is foreseeably going to make them more vulnerable in the future*. Only by ending the collection of sensitive biometric and personal data is it possible to address the real harms of surveillance technology on the people of New York.

New Yorkers Do Not Want to be Surveilled

Time and again, the people of New York City have made clear that they value their privacy and do not want to be surveilled by *anyone*. Beginning with executive orders in 1989 and 2003, New Yorkers demonstrated their commitment to ensuring that their private data is not shared with federal immigration authorities.[47] These orders have been reinforced by the City Council five separate times over the last 15 years.

In 2011, the Council restricted the Department of Corrections from cooperating with federal immigration detainers.[48] In 2013, the Council implemented similar limitations on cooperating with immigration detainers for the NYPD.[49] In 2014, the Council further restricted the NYPD's involvement with federal immigration officials as soon as it was apparent that it could do so lawfully.[50] Finally, in 2017 the Council passed two more bills limiting cooperation with federal immigration officials: the first restricted all government agencies from spending resources to assist immigration policing;[51] the second significantly limited access to city property by all types of federal policing agencies.[52] Each of these efforts was designed to ensure that personal information was not being transmitted or shared with federal authorities.

New Yorkers' desire for privacy extends beyond immigration policing, as similar laws have expressed communities' desire not to be surveilled by local government or private businesses either. New Yorkers

---

[46] Masha Borak, *US Bid for Dutch Digital ID Infrastructure Company Raises National Security Fears*, Biometric Update (Jan. 26, 2026), https://www.biometricupdate.com/202601/us-bid-for-dutch-digital-id-infrastructure-company-raises-national-security-fears (showcasing the risk of sensitive data being acquired by foreign corporations).

[47] NEW YORK CITY DEPARTMENT OF INVESTIGATION, DOI Investigation into the NYPD's Compliance with Local Laws Restricting City Assistance with Immigration Enforcement, Release #49-2025, (Dec. 3, 2025), https://www.nyc.gov/assets/doi/reports/pdf/2025/49NYPD.SancLawsRelease.Rpt.12.03.2025.pdf

[48] Local Law 2011/062, https://intro.nyc/local-laws/2011-62; *see also* N.Y. City Admin. Code § 9-131 (as amended)

[49] Local Law 2013/021, https://intro.nyc/local-laws/2013-21; *see also* N.Y. City Admin. Code § 14-154 (as amended)

[50] Local Law 2014/059, https://intro.nyc/local-laws/2014-59; New York City Council, Press Release, *Council to Vote on Legislation Banning Warr*[*a*]*ntless ICE Detainers* (Oct. 22, 2014), https://council.nyc.gov/press/2014/10/22/314/

[51] https://intro.nyc/local-laws/2017-228

[52] Local Law 2017/246, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3022111&GUID=2471E159-AF64-4416-801A-91321D8D281E&Options=ID|Text|&Search= [accessible as a PDF by clicking hyperlink "Local Law 246"]; *see also* N.Y. City Admin. Code § 4-210

have taken stands against municipal agencies through the adoption of municipal data privacy legislation enacted in 2017,[53] against local law enforcement through the 2020 POST Act and its 2025 expansion,[54] and against their landlords through the 2021 Tenant Data Privacy Act.[55] At the state level, New Yorkers also expressed concern about the way private businesses handle and use their data by enacting the SHIELD[56] and the New York Algorithmic Pricing Act.[57] New Yorkers' willingness to fight for each of these bills year after year sends a clear message: *stop stealing our data*.

Despite these repeated attempts from New Yorkers to secure their personal and private data, their desire for privacy has been undermined by key limitations in law and administration. For instance, the New York City administrative code's regulations on municipal agency data sharing allow the police to collect, receive, or disclose data virtually at will.[58] Other municipal agencies are held to similarly minimal standards, as is evident through past programs like Worker Connect.[59] Current laws also only allow for a maximum of $5,000 in damages; given the difficulty of determining if your personal information has been sold and the costs of bringing an individual suit, this does not serve to adequately disincentivize businesses from selling personal data. Moreover, biometric data is unique, meaning once it is leaked it may well never be recoverable, further showing that proactive (as opposed to a reactive) regulations are needed to meaningfully secure private data. Appealing digital theft of one's likeness, as we can tell from the ongoing weaponization of deep fakes, is too much burden to add to already burdened New Yorkers.

Beyond just the structural and technical limitations of the laws adopted by the city, compliance has also been lackluster. New York Department of Investigation reports have found that the NYPD repeatedly flouts both the POST Act[60] and limitations on cooperation with federal immigration enforcement.[61] New Yorkers fought hard to get these laws passed, and they expect restraints on surveillance and data collection in

---

[53] N.Y. City Admin. Code, §23-1201 *et seq.* (L.L. 2017/247, 12/17/2017, eff. 6/15/2018; Am. L.L. 2023/061, 5/26/2023, eff. 11/22/2023)

[54] Local Law 2020/065; N.Y. City Admin. Code, § 14-188; N.Y. City Charter, § 803. *See also* New York City Council, Press Release, *City Council Passes Expanded POST Act Legislative Package to Strengthen Transparency and Oversight of NYPD Surveillance Technology* (Apr. 15, 2025) https://council.nyc.gov/amanda-farias/2025/04/15/city-council-passes-expanded-post-act-legislative-package-to-strengthen-transparency-and-oversight-of-nypd-surveillance-technology/

[55] N.Y. City Admin. Code, § 26-3001 *et. seq.*

[56] https://www.nysenate.gov/legislation/bills/2019/S5575

[57] N.Y. Gen. Bus. Law § 349-A

[58] *Supra* note 49, § 23-1202

[59] Anemona Hartocollis, *Concern for Vast Social Services Database on the City's Neediest*, NEW YORK TIMES, (Jun. 16, 2011), https://www.nytimes.com/2011/06/17/nyregion/promise-and-concern-for-vast-social-services-database-on-citys-neediest.html?searchResultPosition=1 (examining the risks of the Worker Connect database)

[60] NEW YORK CITY DEPARTMENT OF INVESTIGATION, An Assessment of NYPD's Compliance with the POST ACT, Release #45-2024, (Nov. 26, 2024) https://www.nyc.gov/assets/doi/reports/pdf/2024/49PostActRelease.Rpt.12.18.2024.pdf

[61] NEW YORK CITY DEPARTMENT OF INVESTIGATION, DOI Investigation into the NYPD's Compliance with Local Laws Restricting City Assistance with Immigration Enforcement, Release #49-2025, (Dec. 3, 2025), https://www.nyc.gov/assets/doi/reports/pdf/2025/49NYPD.SancLawsRelease.Rpt.12.03.2025.pdf

return.[62] Instead, they have been faced with increased usage of facial recognition and other surveillance technologies in their day-to-day lives, both from law enforcement and private businesses. To honor New Yorkers' expectations, the Council should effectuate a strong and comprehensive system that cuts off the harm of surveillance at the source: the surveillance itself.

Surveillance by retail or grocery[63] stores, or other places of public accommodation,[64] is just as unpopular as surveillance by law enforcement.[65] And as if it were not harmful enough on its own, biometric collection and recognition technologies deployed in places of public accommodation also increases law enforcement agencies' ability to acquire sensitive data, as there are no restrictions on a private business selling or sharing biometric data with the police.[66]

New Yorkers are not interested in being asked for their informed consent before being surveilled, they *do not want to be surveilled at all*. In recognition of this, the New York State Legislature has introduced numerous bills seeking to curtail the use of surveillance technology, including the New York Data Protection Act,[67] the Protecting Consumers and Jobs from Discriminatory Pricing Act,[68] and more.[69] The efforts are community- and worker-driven, reflecting the importance of surveillance technology to the people of New York.[70]

Current Data Privacy Laws Do Not Adequately Protect New Yorkers

Current data privacy laws focus primarily on what happens to personal data *after* it is collected, rather than preventing people's private information from being harvested in the first place. It also centers the direct

---

[62] New York City Council, Press Release, *City Council Passes Expanded POST Act Legislative Package to Strengthen Transparency and Oversight of NYPD Surveillance Technology* (Apr. 15, 2025) https://council.nyc.gov/amanda-farias/2025/04/15/city-council-passes-expanded-post-act-legislative-package-to-strengthen-transparency-and-oversight-of-nypd-surveillance-technology/

[63] Liam Quigley, *NYC Wegmans Is Storing Biometric Data on Shoppers' Eyes, Voices and Faces*, GOTHAMIST (Jan. 3, 2026), https://gothamist.com/news/nyc-wegmans-is-storing-biometric-data-on-shoppers-eyes-voices-and-faces

[64] Jacob Sowers, *Madison Square Garden's Use of Facial Recognition Technology to Bar Certain Lawyers Stirs Protests*, FREE SPEECH PROJECT AT GEORGETOWN UNIVERSITY, (Jul. 18, 2023), https://freespeechproject.georgetown.edu/tracker-entries/madison-square-gardens-use-of-facial-recognition-technology-to-bar-certain-lawyers-stirs-protests/

[65] Paige Oamek & Andrew Giambrone, *Not Just Wegmans: More NYC Retailers Using Facial Recognition as Tech Outpaces Law*, GOTHAMIST (Jan. 12, 2026), https://gothamist.com/news/not-just-wegmans-more-nyc-retailers-using-facial-recognition-as-tech-outpaces-law

[66] N.Y. City Admin. Code, §22-1201 *et seq.* (L.L. 2021/003, 1/10/2021, eff. 7/9/2021) (exempting biometric identifier information "shared with, sold or leased to . . . law enforcement agencies" from regulatory requirements).

[67] Senate Bill S4860 (establishing the New York Data Protecting Act), https://www.nysenate.gov/legislation/bills/2025/S4860

[68] Senate Bill S8616 (establishing the Protecting Consumers and Jobs from Discriminatory Pricing Act), https://www.nysenate.gov/legislation/bills/2025/S8616

[69] Senate Bill S8623, https://www.nysenate.gov/legislation/bills/2025/S8623 (banning the use of personal data to algorithmically set prices)

[70] Johan Sheridan, *New York Democrats Want to Ban Surveillance Pricing, Digital Price Tags*, NEWS10, (Feb. 11, 2026), https://www.news10.com/capitol/new-york-democrats-want-to-ban-surveillance-pricing-digital-price-tags/

identification of individuals and shows little concern for the damage that data can do when aggregated. When not directly regulating the handling of personal data, local laws operate mainly to ensure that individuals are informed that they are being surveilled or through securing their consent. None of these approaches are especially effective at restraining the state and corporate surveillance making New Yorkers vulnerable to surveillance pricing and policing.

First, nothing in the current municipal laws forbids an establishment from collecting and using people's personal data for its own ends. Rather, municipal law[71] only forbids establishments from selling or trading information to third parties. Concerningly, it also appears that the current law allows companies to simply *give away* personal data.[72] As a result, establishments are free to collect and weaponize people's own data against them as much as they want, with the only caveat being that they cannot outsource such exploitation to other companies.

But with an increasing number of private businesses conducting their own surveillance,[73] limiting disclosures in this way hardly reduces how frequently people's data is being used against them. It also does little to guard against the risk that the data will be stolen or mishandled; the vast proliferation of people's data means that even with reasonable security measures in place[74] there is still a significant risk of disclosure or breach. It also ignores the powerful incentive of private corporations to sell the data illicitly to massive data-hungry corporations (particularly those operating in the sphere of Artificial Intelligence) who seek to develop myriad systems that turn people's own data against them.

Second, statutorily requiring the posting of notices or otherwise asking for legal consent allows corporations to take advantage of their market position in comparison to consumers, tenants, and workers.[75] New Yorkers can hardly afford—either in terms of time or money—to search high and low for the one grocery store that is not scanning them while they shop. Worse, it is likely that such a grocery store will not exist in the near future, leaving consumers and workers with no practical choice but to submit to being surveilled. This is not consent, and it is not privacy.

New Yorkers should be free to shop wherever they want without worrying about being watched; the only way to accomplish that is to prevent surveillance technology from being deployed in shops, stores, and businesses across the city. Doing so will also protect New Yorkers from being targeted by data-mining

---

[71] N.Y. City Admin. Code § 22-1202(b)

[72] Emile Ayoub & Elizabeth Goitein, *Closing the Data Broker Loophole*, BRENNAN CENTER FOR JUSTICE, (Feb. 13, 2024), https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole (explaining how companies might circumvent exchange limitations in data privacy laws)

[73] U.S. GOVERNMENT ACCOUNTABILITY OFFICE, *Consumer Data: Increasing Use Poses Risks to Privacy*, (Sep. 13, 2022), https://www.gao.gov/products/gao-22-106096 (noting a massive increase in consumer surveillance in recent years)

[74] For example, those mandated under the SHIELD Act. N.Y. Gen. Bus. Law § 899-bb; *see also* Senate Bill 5575, https://www.nysenate.gov/legislation/bills/2019/S5575

[75] Claire Park, *How "Notice and Consent" Fails to Protect Our Privacy*, OPEN TECHNOLOGY INSTITUTE, (Mar. 23, 2020), https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/#:~:text=Put%20simply%2C%20notice%20and%20consent,and%20utilizing%20their%20personal%20data.

companies seeking to extract personal information so that they can sell it back to the city[76] and profit twice from the same invasion of privacy.

Third, current privacy laws are difficult to enforce in comparison to a simple ban on biometric collection and surveillance technology. Instead of attempting to track and monitor every sale and transfer of data, it has been long understood that minimizing the amount of data collected is the best and easiest way to protect personal privacy.[77] Adopting a prevention-based approach is thus not only more faithful to what people want, but it is also likely to be cheaper, easier to administer, and more effective.

The Legislation Does Not Adequately Address the Harms of Data Surveillance and AI

Though the legislation prohibits the current use of biometric data recognition technology, it does not adequately address the inherent harms of biometric data collection or target the harms that will arise from future developments of these technologies. By only seeking to prevent the harms that biometric data recognition technology perpetuates now, we fail to see and address the full scope of harm these technologies perpetuate. Incoming threats from agentic AI and identity verification technologies, such as those in the financial technology industry, the education technology industry, and more, must be addressed by this legislation to best protect the identities of New Yorkers and prevent further chaos and infringement upon the privacy rights of all New Yorkers.

Proposed Changes to Int 0213-2026 and Int 0428-2026

Banning the Collection of Biometric Data Would Better Protect Data Privacy

We would encourage a prohibition on biometric data collection, not simply the use of biometric recognition technology. We appreciate the outright ban on the use of biometric recognition technology ("It shall be unlawful for any place or provider of public accommodation to use any biometric recognition technology to verify or identify a customer"[78]), which helps further the purpose of protecting the privacy of New Yorkers. However, the bill currently allows for the the collection of biometric data via an informed consent framework, noting that "Any [commercial establishment]... that collects, retains, converts, stores, [or] shares, or otherwise obtains biometric identifier information of customers must disclose such collection, retention, conversion, storage, [or] sharing, or obtaining of biometric identifier information… by placing a clear and conspicuous sign near all… entrances… and shall be required to get the written consent of such customer in advance of any collection."[79]

---

[76] Pakzad, R., & Conti-Cook, C., *Key Considerations When Procuring AI in the Public Sector*, TARAAZ & THE COLLABORATIVE RESEARCH CENTER FOR RESILIENCE (CRCR), (Aug. 5, 2025), https://taraazresearch.org/ai-procurement (detailing the exploitation of municipal procurement processes by data companies)

[77] ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), *Data Minimization*, https://epic.org/issues/consumer-privacy/data-minimization/ (last accessed Mar. 1, 2026) (explaining the benefits of a data minimization approach)

[78] Int. No. 213, line 19-20

[79] Int. No. 213, line 9-18

A ban on the collection of biometric data at the source would help prevent future threats to data privacy, not just immediate ones. Without a ban on biometric data collection, there is an ever-present risk that either the collector of the data, or a third party with nefarious intent, could access the data without the consumers' consent. Allowing collection, even while outlawing recognition software, still sets up a system where the data might be utilized down the line, even if the collector of the data creates a policy with a "retention schedule and guidelines for the permanent destruction" of the data.[80] Including an outright prohibition on collection would help to ensure that New Yorkers are adequately protected in an ever-evolving technological field that poses continuous surveillance and privacy threats.

In addition, the bill seeks to regulate the collection of biometric data through the implementation of an informed consent scheme, specifying that businesses "shall be required to get the written consent of [customers] in advance of any [biometric data] collection."[81] Implementing an informed consent program might help prevent biometric data collection on an individual level by allowing each consumer to provide consent to the collection of their data. However, the protection of data privacy is not an individual question, but one that applies to all of us. For example, biometric data has the potential to implicate family members of the individual whose data is obtained because it includes genetic identifiers.[82] In that vein, informed consent on an individual level is ineffective to get at the underlying problem of biometric data collection and recognition technology, which is the use of data in enabling more harmful and hostile technologies in the future. Banning collection at the source would undercut these serious security risks, privacy concerns, and protect vulnerable communities by preventing community mapping.

The "informed consent" procedure in the bill also raises key concerns. There exist inherent power dynamics in situations of urgency, whether it is somebody trying to get into their building quickly or someone trying to buy groceries. Those in power (e.g., landlords, businesses, etc.) are able to exploit this urgency in order to obtain consent from those who may otherwise prefer to withhold consent. There also exists a lack of transparency around how individual biometric data will be used, making this inherently different from a situation where somebody is consenting to data sharing with full information. The inherently coercive nature of the situations where biometric data is being collected renders the "informed consent" scheme ineffective.

The Ban on the Sale of Biometric Data Should Extend to Law Enforcement Agencies

We would also encourage extending the ban on the sale of biometric data to government agencies, including police agencies.[83] The bill currently reads, "Nothing in this chapter shall apply to the collection, storage, sharing or use of biometric identifier information by government agencies, employees or agents."[84]

---

[80] Int. No. 213, line 3-4

[81] Int. No. 213, line 17-18

[82] https://www.thehortongroup.com/resources/understanding-the-risks-of-collecting-biometric-data-in-logistics-and-moving-amp-storage/

[83] Int. No. 213, line 17-18

[84] Int. No. 213, line 14-18

Allowing government agencies, including police, to continue using biometric data and recognition technology only serves to further the harms outlined above. Facial recognition technology in particular poses an immediate and substantial threat if biometric data is sold to police agencies. Police departments across the country, including in New York, utilize facial recognition technology by submitting "photos of unknown individuals."[85] The use of technology in attempting to identify suspects does not stop here, though, as police departments often use other software in conjunction with facial recognition technology to edit photos or fill in "missing pieces."[86] This amounts to the utilization of a few pieces of biometric data to fabricate the rest, which results in large errors in outputs.[87] Using "... these techniques to identify criminal suspects, who may be deprived of their liberty and ultimately prosecuted based on the match…" should be unequivocally discouraged.[88] Including police agencies in the ban on the sale of data would serve to better protect the New York community from unfair targeting.

Remedies for Victims are Inadequate, and Government Roles with Responsibility for Decisions Related to Procurement of Technology Should Be Reported On Annually

Finally, we would encourage a more robust system for victims of biometric data collection or recognition technologies to seek remedies for violations. The bill currently prevents raising a claim against the collector of the data if the violation has been "cured" within 30 days.[89] "Curing" a data violation is a misnomer because once the data has been collected and disseminated (whether intentionally or unintentionally), the data is out of the hands of either the individual or the company that collected it, and it can be used by whoever manages to access it.[90]

As such, it is imperative that the responsibility for collection, dissemination, and use of biometric data begins at the stage of procurement. The government actors responsible for each phase of the procurement decision-making process should be clearly identified and their understanding of whether a technology foreseeably increases any risk of constitutional violations must be produced in a written analysis and made publicly available. Instead of placing an undue burden on business owners who may be unable to fully protect the data they collect, transparency and accountability at the stage of procurement would better serve to protect New Yorkers from having their biometric data shared down the line.

---

85 https://www.flawedfacedata.com/

86 *Id.*

87 *Id.*

88 *Id.*

89 Int. No. 213, line 15-22

90 https://jamiejbartlett.substack.com/p/what-actually-happens-to-your-stolen

Conclusion

We testify in support of both bills limiting biometric recognition technology but urge the Council to expand such limitations to ban biometric *collection* technology in addition to *recognition* technology. We also encourage all reporting and use limitations to apply equally to all agencies, including police.

We urge the Council to consider not just the direct harms of surveillance policing but of the community harms–including the potential for taxpayers to have to pay three times for new technologies–for the harm, to compensate for the harm, and for the vendors' service.

At the very least we must have a moratorium on all government procurement of biometric collection and recognition technology, more expansive limitations on insurance policies that pressure businesses to install biometric technologies and limitations on businesses' collection of biometric data.

Adam Scott Wandt, JD, MPA
Associate Professor of Public Policy
Deputy Chair of Technology
awandt@jjay.cuny.edu
https://wandt.us

Testimony of Associate Professor Adam Scott Wandt, J.D., M.P.A
John Jay College of Criminal Justice, The City University of New York

Before the New York City Council Committee on Technology
Regarding Int. 0428-2026 and Int. 0213-2026:
Facial Recognition Technology and the Protection of Biometric Data

March 2026

Chairpersons, Council Members, and Members of the Public:

Thank you for the invitation and opportunity to testify today. My name is Professor Adam Scott Wandt, and I serve as Associate Professor of Public Policy and Deputy Chair for Technology within the Department of Public Management at John Jay College of Criminal Justice. A great deal of my academic and professional work focuses on the intersection of law, technology, and government transparency. I am also a licensed and practicing attorney, and former co-chair of the New York City Bar Association's Committee on Technology, Cyber and Privacy Law. I am a member of the Board of Directors of the Association of Inspectors' General, where I work to increase the technology and cyber knowledge levels of our inspection and oversight professionals. I have spent nearly two decades researching and advising on digital policy initiatives to increase public trust, accountability, and access to government services. My complete biography is available on my website: wandt.us. My comments are my own and do not reflect the official position of any organization with which I am affiliated.

I am here in strong support of both Int. 0428-2026 and Int. 0213-2026.

Let me be clear at the outset: facial recognition technology is not inherently bad. In law enforcement, in national security, and in controlled high-security settings with proper oversight, it can be a valuable tool. But there is a profound difference between targeted, supervised use and the widespread, routine deployment of biometric surveillance in the places where New Yorkers live, shop, eat, and go about their daily lives. That widespread deployment carries real costs to privacy, security, and civil liberties, and these two bills address those costs head-on.

Turning first to **Int. 0428-2026**, which would ban facial recognition in residential buildings: your home is the most private space you occupy. Allowing landlords to deploy facial recognition at building entrances creates a persistent record of every tenant's movement, when they leave, when they return, and who visits them. That is not a security system. That is a surveillance infrastructure.
And here is the core problem: this data cannot be kept safe. Facial recognition data is fundamentally different from a password or a credit card number. If those are stolen, you change them. But you cannot change your face. Once your faceprint is exfiltrated, the damage is permanent.

This is certainly not theoretical. Clearview AI had over three billion facial images breached. The U.S. Office of Personnel Management lost fingerprint data for 5.6 million federal employees from a government database that met federal security standards. The Biostar 2 platform exposed 27.8 million biometric

records in an unencrypted, publicly accessible database. If the federal government and major security firms cannot protect this data, we should not expect a building management company to do better.

Beyond breaches, there is the risk of monetization. Data brokers have built multi-billion-dollar industries on data people never knowingly shared. A facial recognition vendor servicing an apartment building accumulates the biometric identities and movement patterns of potentially millions of New Yorkers. The temptation to sell that data is enormous—and corporate acquisitions and bankruptcies can transfer it to entities with very different intentions.

My one concern with this bill is enforcement. A prohibition without teeth risks becoming aspirational. Tenants need a clear path to remedy, a private right of action, a designated enforcement agency, or both, and the Council should consider periodic auditing requirements for large housing complexes.

Turning to **Int. 0213-2026**: This bill's expansion from "commercial establishments" to all places of public accommodation is exactly right. It closes gaps that left gyms, medical offices, coworking spaces, and houses of worship unregulated. The mandatory written consent requirement, the prohibition on selling biometric data, the right to erasure, and the private right of action are all strong, well-crafted provisions. My concern here is the penalty structure. At $500 per negligent violation and $5,000 per intentional violation, a major retailer or entertainment venue may simply treat these fines as a cost of doing business. The Council should consider tiered penalties based on entity size or data volume, so the law has teeth for everyone, not just small businesses.

In closing, these bills are grounded in the principles that should guide all technology regulation: transparency, enforcement, and oversight. They recognize that limiting the collection of biometric data is the most effective way to protect it. I urge the Council to pass both bills, and I am happy to answer any questions.

Thank you.

Adam Scott Wandt

NYC | HOSPITALITY ALLIANCE

March 2, 2026

Testimony of the New York City Hospitality Alliance to the New York City Council's Committee on Technology on Introduction 0213-2026: Prohibiting places or providers of public accommodation from using biometric recognition technology and protecting any biometric identifier information collected

On behalf of the New York City Hospitality Alliance, a nonprofit trade association representing thousands of restaurants, bars, and nightclubs across the five boroughs, we submit testimony for your consideration related to Introduction 0213-2026.

Biometric recognition technology raises concerns around surveillance, misuse, and discriminatory impacts. Establishing clear guardrails for places of public accommodation is an important and timely policy endeavor. At the same time, because the bill adopts a broad definition of "place or provider of public accommodation," it will apply to nearly every consumer-facing hospitality business in New York City. For the restaurants, bars, nightlife venues, hotels, music venues, and event spaces we work with and represent, several provisions warrant careful consideration.

First, the bill creates a flat prohibition on the use of biometric recognition technology to verify or identify customers. In practice, this would prohibit facial recognition systems used to identify banned patrons, manage trespass lists, or streamline entry for members-only venues. While many operators do not currently use these tools, some larger nightlife venues have explored them as safety mechanisms to prevent repeat violent incidents.

Nightlife venues, in particular, operate in environments where crowd management and patron safety are serious responsibilities. As policymakers consider this legislation, we encourage discussion around how privacy protections can be balanced with legitimate safety concerns, especially in high-capacity venues that must manage risk in real time.

Second, the bill expands compliance obligations and creates significant litigation exposure through a private right of action, including statutory damages and attorneys' fees. For high-volume establishments serving hundreds or thousands of guests per week, even inadvertent or vendor-driven violations could create substantial liability. Many hospitality businesses rely on third-party point of sale (POS) systems, security vendors, and AI-enabled camera systems. Operators may not always know whether embedded features qualify as biometric recognition under the bill's definitions.

NYC | HOSPITALITY ALLIANCE

Clarity around scope, vendor responsibility, and what constitutes “use” will be critical to ensuring that businesses can comply without facing disproportionate legal risk.

Third, as drafted, the bill may impede future technological developments that could serve legitimate purposes. Biometric tools are evolving rapidly, and new applications could include privacy-respecting age estimation, opt-in loyalty recognition, seamless payment authentication, or accessibility support for guests with disabilities. While many of these technologies are still emerging, a blanket prohibition on identification uses, even if consent-based, may limit innovation that could ultimately benefit both consumers and businesses.

As the Council advances this legislation, we respectfully encourage careful consideration of several implementation questions. Clarifying the distinction between identifying a specific individual and the use of anonymized or non-retentive tools would help avoid unintended consequences for routine hospitality operations. Thoughtful examination of how high-capacity venues are expected to address repeat safety risks without technological tools would also provide important guidance to operators responsible for managing large crowds.

In addition, ensuring that liability is appropriately allocated between businesses and third-party vendors, particularly where biometric features may be embedded in security or POS systems, will be critical for small and mid-sized establishments that lack in-house compliance resources. Finally, given the bill’s private right of action and per-violation damages, calibrating enforcement to promote good-faith compliance without exposing neighborhood businesses to disproportionate legal risk will be important.

New York City’s hospitality industry is committed to welcoming guests in ways that are safe, inclusive, and respectful of privacy. We look forward to working with the Council to ensure that this proposal protects both civil liberties and reflects the operational realities of restaurants, bars, and nightlife venues across the five boroughs.

NYCLU
ACLU of New York

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

Testimony of Medha Raman

On Behalf of the New York Civil Liberties Union

Before the New York City Council Committee on Technology in Support of Intros. 213 and 428

March 2, 2026

The New York Civil Liberties Union ("NYCLU") respectfully submits the following testimony regarding the oversight and use of biometric identification systems in New York City. The NYCLU advances civil rights and civil liberties so that all New Yorkers can live with dignity, liberty, justice, and equality. Founded in 1951 as the state affiliate of the national ACLU, we deploy an expert mix of litigation, policy advocacy, field organizing, and strategic communications. Informed by the insights of our communities and coalitions and powered by 90,000 member-donors, we work across complex issues to create more justice and liberty for more people. The NYCLU works to expand the right to privacy, increase the control individuals have over their personal information, and ensure civil liberties are enhanced rather than compromised by technological innovation.

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

The Council must ensure New Yorkers are not surveilled, targeted, discriminated against, and criminalized on the basis of invasive, flawed, and biased technology. To this end, we call for prohibitions on biometric surveillance in areas of severe power imbalance, including its use by law enforcement or other government agencies, in housing, and in other areas where our fundamental rights are at stake or where informed consent cannot be given. The NYCLU supports the two bills before the Committees, Introduction 213-2026, which would ban biometric surveillance in places of public accommodation and set clear rules for the collection of biometric data, and Introduction 428-2026, which would ban the use of biometric surveillance in residential buildings.

Biometric Surveillance Has No Place in New York City

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

The widely reported deployments of facial recognition at Madison Square Garden to ban people from the stadium who had already purchased tickets[3] and at Wegmans to collect information on shoppers[4] illustrate the dangers from the growing surveillance industry and the urgent need for comprehensive privacy protections. And the planned installation of a facial recognition entrance system at the Atlantic Plaza Towers in Brownsville raised severe concerns about imposing invasive surveillance on residents and their guests.[5] Fortunately, the tenants were successful in their advocacy against the landlord's plan and were able to stop the system from being deployed. Such a system raises significant concerns about misidentifications resulting in potentially dangerous interactions, privacy violations by precisely tracking the

---

[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*, N.Y. 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] Liam Quigley, *NYC Wegmans is storing biometric data on shoppers' eyes, voices and faces*, GOTHAMIST, Jan. 3, 2026, https://gothamist.com/news/nyc-wegmans-is-storing-biometric-data-on-shoppers-eyes-voices-and-faces.

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

coming and going of every resident and their guests, building access issues, and heightened security risks due to the collection of biometric and movement data.

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.[6] Disclosing data policies, setting clear retention and deletion schedules, protecting against any third-party access, and establishing appropriate security mechanisms should be the baseline for anyone handling biometric data.

These risks are even more heightened for immigrant New Yorkers. As the Department of Homeland Security continues to rely on surveillance technologies to target immigrant communities,[7] immigrants live in fear not only in public as they go about their daily lives, but also in their own homes. Once biometric recognition systems collect data, it risks creating and amassing highly personal information that could be exploited by immigration officials. Restricting the use of biometric surveillance technology is an essential step towards protecting New Yorkers from federal overreach.

Introduction 213-2026 - Prohibiting places or providers of public accommodation from using biometric recognition technology and protecting any biometric identifier information collected.

Intro. 213 would amend the biometric disclosure for businesses law (Local Law 3 of 2021), Section 22-1201 of the Administrative Code, to prohibit places or providers of public accommodations from using biometric recognition technology to identify customers, and it would require written consent for any collection of biometric identifier information. It would further create transparency, security, and deletion requirements and ensure that customers are not treated or charged differently because they do not consent to the collection of their biometric data.

These changes add crucial protections to New York City law. As mentioned above, the deployment by MSG Entertainment across its sports and entertainment venues to target staff from law firms in litigation with MSG points to Orwellian use cases where it will be impossible to move and associate freely. And the technology's racial as well as gender bias risks disproportionately impacting women and people of color, such as in the misidentification of a

---

[6] *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.

[7] Steven Hubbard, *ICE Uses a Growing Web of AI Services to Power Its Immigration Enforcement and Surveillance*, AM. IMM. COUNCIL, Dec. 18, 2025, https://www.americanimmigrationcouncil.org/blog/ice-uses-ai-immigration-enforcement-surveillance/.

Black teenager that barred her from entering an skating rink[8] or in that of a woman in the UK who was misidentified as a shoplifter and subsequently bag searched, asked to leave the store, and banned from all stores using the same technology – until the company acknowledged its mistake.[9]

Raising related harms, the Federal Trade Commission successfully brought charges against the large retailer Rite Aid, which is now banned from using facial recognition after similarly falsely identifying consumers as shoplifters.[10] For these reasons, we support banning biometric surveillance in places of public accommodations. Visiting retail stores, restaurants, museums, entertainment venues, or healthcare sites should not automatically open one up for the collection of sensitive biometric information without prior informed consent and clear rules for access, use, security, retention, and deletion. While Local Law 3 of 2021 was a modest first step in addressing use of biometric technologies by businesses, it was nowhere near sufficient. That law merely requires certain "commercial establishments" that collect, use, or retain "biometric identifier information" from their customers to post signs at all entrances. The minimal notice does not include any information about the specific biometric surveillance tools in use or the collected data and further does not require businesses to disclose for what purpose the technology is used, for how long data is retained, with whom data is shared, or how it is secured. The NYCLU has repeatedly testified on this issue at the committee hearing on October 7, 2019, the hearing by the Department of Consumer and Worker Protection on the proposed rules on August 30, 2021, and the Committee on Consumer and Worker Protection on February 24, 2023.

In New York City, Macy's, Fairway, Whole Foods, and most recently, Wegmans, have all disclosed their use of facial recognition technology pursuant to Local Law 3 of 2021.[11] The public backlash to this news demonstrates how the notice requirements under existing law are insufficient to adequately protect the privacy of members of the public who are forced to surrender their biometric data just to buy groceries. Without stronger protections, biometric recognition technology risks creating a constant state of surveillance, wrongly excluding people from public life due to misidentification, and threating New York's immigrant communities if sensitive information is shared with law enforcement.

---

[8] 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.

[9] James Clayton, *"I Was Misidentified as Shoplifter by Facial Recognition Tech,"* BBC, May 25, 2024, https://www.bbc.com/news/technology-69055945.

[10] Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards, Federal Trade Commission (2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without.

[11] Paige Oamek and Andrew Giambrone, *Not just Wegmans: More NYC retailers using facial recognition as tech outpaces law,* GOTHAMIST, Jan. 12, 2026, https://gothamist.com/news/not-justwegmans-more-nyc-retailers-using-facial-recognition-as-tech-outpaces-law.

In addition to its important ban on the use of biometric recognition technologies in places of public accommodations, Introduction 213 would create the needed guardrails and protections for any biometric identifier information that such places of public accommodation may still be permitted to collect. To ensure that the legislation fully meets its goals, we make the following recommendations.

The definition of "customer" remains tied to the to-be-deleted term of "commercial establishment." Instead of merely editing or removing the mention of this term, we recommend utilizing "individuals," "natural person," or other broader and more inclusive terms appropriate for the context in public accommodations throughout the entire bill instead of the narrower term of "customer." The use of "customer" rather than a broader term risks excluding patients and visitors in hospitals or clinics, travelers in train stations, and individuals accessing social services or enjoying public parks.

Section 22-1203 amends the existing private right of action of Local Law 3, which requires prior notice of at least 15 days to violating entities, allowing them to cure the violation within 15 days to prevent further action. Although the amendment ensures that an aggrieved person would not have to provide such notice prior to commencing an action against a place or provider of public accommodation that uses a prohibited biometric recognition technology or that shares, sells, or discloses biometric identifier information, the legislation would require those who have been subject to unconsented biometric data collection to first inform violating entities and allow them 15 days to cure the violation. Such an obligation severely undermines the proposed affirmative written consent protection. The importance of a robust private right of action as an accountability and enforcement tool cannot be overstated, and we strongly urge the Council to strengthen this section to protect against violations.

The NYCLU supports this legislation and urges its passage.

Introduction 428-2024 - Limiting the use of facial recognition technology in residential buildings.

Intro. 428 would prohibit owners of multiple dwellings from installing, activating, or using any biometric recognition technology that identifies tenants or their guests. Such strict limits are necessary because the deployment of biometric surveillance at people's homes raises constitutional concerns and intrudes on tenants' rights of self-determination and privacy. It risks conditioning entry into one's home – the place where our constitutional rights are at their most robust – on the provision of one's most sensitive biological data. Residents should not have to live in fear that landlords are tracking their comings and goings and amassing sensitive data on them and their guests. And those tenants and guests who are women, children, and people of color have particular reason to fear such a change in their housing rights, as facial recognition systems are notoriously inaccurate when it comes to these groups. Thus, not only does biometric surveillance in residential buildings cause harm to tenants' privacy rights, but also their civil rights to access housing on equal and nondiscriminatory terms.

Facial recognition technology has also allowed landlords of rent-stabilized buildings to single out or retaliate against tenants, including by enabling them to spy on tenants to raise their rent, fine them, or evict them for trivial policy violations.[12] One single mother was even targeted after she started night classes and asked her ex-husband to spend more time at her home watching their children, causing her to be flagged for potentially violating the housing authority's visitor policy.[13]

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

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

Biometric Surveillance by Law Enforcement

While the two biometrics bills before the Committees focus on biometric surveillance in places of public accommodations and in residential buildings, we must stress the dangers of biometric surveillance in the hands of government agencies, specifically law enforcement. The New York Police Department ("NYPD") already has more than 20,000 cameras integrated into its Domain Awareness System[14] and plans to increase that number to a staggering 50,000 cameras.[15] In February 2026, NYPD Police Commissioner Jessica Tisch announced the introduction of a Domain Awareness System 2.0, describing the system as providing real-time alerts from surveillance technologies directly to officers in the field.[16] 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

---

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

[13] Douglas MacMillan, *Eyes on the Poor: Cameras, Facial Recognition Watch Over Public Housing*, WASH. POST, May 16, 2023, https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/.

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

[15] Preparedness Grant Effectiveness Case Study: New York City, 27 (2021), https://www.fema.gov/sites/default/files/documents/fema_nyc-case-study_2019.pdf; Zachary Groz, *NYPD Plans Massive Expansion of Real-Time Surveillance in NYCHA Housing*, N.Y. FOCUS, Oct. 1, 2025, https://nysfocus.com/2025/10/01/nypd-nycha-surveillance-hearing.

[16] Press Release, *Commissioner Tisch Announces New Strategies to Keep New Yorkers Safe, Improve Officer Training, and Modernize Policing*, N.Y.P.D., Feb. 10, 2026, https://www.nyc.gov/site/nypd/news/PR003/commissioner-tisch-new-strategies-keep-new-yorkers-safe-improve-officer-training-and.

recognition software to identify a Black Lives Matter activist during a protest against police brutality through a photo from his Instagram account.[17]

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.[18]

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.[19]

The real risks of misidentification by law enforcement cannot be overstated, especially considering the potential for lifelong consequences that can result from even a single encounter with law enforcement.[20] In April 2025, Trevis Williams—a 6'2", 230-pound Black man—was wrongfully arrested by the New York Police Department (NYPD) for indecent exposure, accused of a crime committed by someone eight inches shorter and 70 pounds lighter.[21] Despite location data showing he was miles away at the time, a faulty facial recognition match landed him behind bars for more than two days.[22] Williams's life and job prospects were put on hold for months due to his false arrest.

---

[17] 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.

[18] 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).

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

[20] See, e.g., Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES, June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES, December 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[21] Maria Cramer & Kashmir Hill, *How the N.Y.P.D.'s Facial Recognition Case Fell Apart*, N.Y. TIMES, Aug. 26, 2025, https://www.nytimes.com/2025/08/26/nyregion/nypd-facial-recognition-dismissed-case.html.

[22] *Id.*

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.[23] And despite the NYPD's explicit rejection, citing concerns about security and the potential for abuse, of software developed by Clearview AI that scrapes billions of photographs from social media platforms and other public sources, it has been reported that dozens of "rogue" officers have continued to use the software in more than 11,000 searches.[24] The reporting noted that "[i]t is not clear if the NYPD officers will face any disciplinary action for using the app,"[25] 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 has also attempted to circumvent existing restrictions on the use of Clearview AI's facial recognition technology by outsourcing requests to other city agencies, such as the FDNY.[26] 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 50 billion facial images – biometric data on virtually everyone who has ever uploaded photos to Facebook, Instagram, Twitter, Venmo, or other social media platforms.[27]

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

---

[23] 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.

[24] *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.

[25] *Id.*

[26] *See* Samantha Maldonado, *NYPD Bypassed Facial Recognition Ban to ID Pro-Palestinian Student Protester*, THE CITY, (Jul. 18, 2025), https://www.thecity.nyc/2025/07/18/nypd-fdny-clearview-ai-bancolumbia-palestinian-protest/; *People v. Zuhdi A.*, No. CR-017044-24NY (Crim. Ct. Jun. 17, 2025), available at https://www.nycourts.gov/reporter/3dseries/2025/2025_51047.htm#:~:text=The%20defendant%20was%20identified%20in%20early%20June%202024,to%20dismiss%20the%20felony%20on%20September%2023%2C %202024.

[27] *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*, N.Y. TIMES, Jan. 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; and Chris Burt, *Clearview facial recognition searches double, database reaches 50B images*, BIOMETRICUPDATE, Jun. 26, 2024, https://www.biometricupdate.com/202406/clearview-facial-recognition-searches-double-database-reaches-50b-images.

in the transit system.[28] 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.[29] 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."[30] Studies have shown that affect recognition and suspicious behavior detection tools overpromise on their capabilities and are severely inaccurate and plagued by racial bias.[31]

Correctional facilities have also become a testing ground for biometric surveillance technologies. The New York Department of Corrections and Community Supervision ("DOCCS") uses facial recognition for "visitation processing," deploying it to deny visitation to family members, friends, and other loved ones who wish to visit people in DOCCS's custody.[32] 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.[33] In March 2021, it was revealed that a vendor recorded confidential attorney-client calls and provided them

---

[28] 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/.

[29] 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.

[30] 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.

[31] *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.

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

[33] *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).

to New York City district attorneys.[34] An audit disclosed that nearly 2,300 calls to attorneys were recorded.[35]

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

Conclusion

In conclusion, the NYCLU thanks the Committees on Technology and on Civil and Human Rights for the opportunity to provide testimony and for their oversight of biometric surveillance in New York City. Nobody wants to live in world where pervasive surveillance identifies them, tracks their movements and associations, and impacts which places they can visit, which services they can access, with whom they meet, or how they exercise their free speech rights. The NYCLU supports Introductions 213-2026 and 428-2026 and we urge their swift passage.

---

[34] 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.

[35] 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.

March 2, 2026

The Honorable Carmen De La Rosa
Chair
Committee on Technology
New York City Council
New York, NY

Written Testimony of the Security Industry Association for Committee on Technology Hearing, "Oversight - Facial Recognition Technology and the Collection of Biometric Data"

Dear Chair De La Rosa and Members of the Committees:

On behalf of Security Industry Association (SIA), a nonprofit trade association representing more than 80 companies headquartered in New York State and 1,600 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 throughout the U.S. Among these are the leading providers of biometric technologies used in a wide variety of government, commercial and consumer products.

Today, biometric technologies contribute to the safety and security of our communities and bring value to our daily lives. At the same time, it's critical that advanced technologies – including biometrics – are used in a secure manner and only for purposes that are lawful, ethical, and nondiscriminatory.[1] While we support polices that would help ensure responsible and effective use of such technologies, we have serious concerns with the two proposals relating to biometric technologies being discussed at today's hearing, Int. 213-2026 (Hanif)[2] and Int. 428-2024 (Sanchez).[3]

Blanket Ban on use of Biometric Technologies by Businesses, Customers

As drafted, Int. 213 would simply outlaw most uses of biometric technologies by businesses and consumers regardless of the purpose or whether it is part of a service requested or agreed to by an individual. This would (1) rob consumers of the choice to use more secure and convenient methods to verify their identity and (2) dictate unnecessary limitations on methods New Yorkers can use to protect themselves and their property.

Commercial/Consumer Applications: Biometric technologies are extensively used in commerce and by business throughout New York City. The enactment of such proposals would not only force businesses to

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

[2] https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=7861954&GUID=1D5898C5-53CA-49DA-BA41-84EF0DD03FC3&Options=ID%7CText%7C&Search=biometric

[3] https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=7862812&GUID=82868853-7D34-466F-B2FD-0617D9CF75DC&Options=ID%7CText%7C&Search=biometric

scrap hardware and software in which significant investments have been made, it would directly harm consumers. Here are just a few examples of the beneficial applications of biometric technology that would be eliminated:

- Biometrically secured user authentication for account access and payment to a business, whether online or in-person.
- App-based accounts and payment systems utilizing biometric customer authentication on electronic devices.
- Customer choice of biometric verification as a more convenient form of payment and access at sporting events and other entertainment venues.
- Convenient fingerprint or face access provided to gym members.
- Use of biometrics for streamlined embarkation on cruise ships, and seamless "curb-to-gate" travel experiences at airports.
- Biometrically enabled security systems protecting persons or property, including systems augmenting efforts to fight organized retail crime.

The proposed prohibition would also be applicable to a wider range of businesses than New York City's the existing biometric data ordinance, which would now include any *"place or provider of public accommodation."* Many businesses will undoubtedly be caught unaware and subjected to litigation over such a sweeping prohibition, as it is authorized in the underlying Biometric Identifier Information Law,[4] and biometric technologies are so thoroughly embedded throughout common commercial applications and operational systems. This mechanism will result in significant legal action, liability and settlements over alleged violations (versus actual consumer harms).

And even then, we can expect many of these suits will be frivolous, based on experience with the class action lawsuits filed under the City's existing law since it went into effect in 2021. All of these were dismissed after Courts found no evidence of viable claims. We also highlight the devastation to businesses in Illinois stemming from the Illinois Biometric Data Protection Act (BIPA) – which notably does not outright prohibit all use of biometric technologies but uses a similar enforcement mechanism for its requirements via private right of action. BIPA lawsuits have mostly involved non-controversial uses of biometrics. 88% of the cases have been related to biometric timekeeping for hourly employees to clock in to work. 20% of cases actually alleging consumer harm have included the use of virtual try-on services, and 40% have involved security and identity verification services.[5] Notably, in 2024, the Illinois legislature amended this law to limit total per-person awards, in order to help stem the tide of frivolous class action lawsuits under BIPA.

Additionally, we are concerned that the proposal expands the scope of what is defined as *"biometric identifier information"* to information that is not, in fact, biometric. As proposed, this would include any identifying characteristic that can be used *"in combination...with other information"* to establish individual identity, which potentially covers a wide range of non-biometric information that is commonly accepted, such as photos or unique identification numbers. Enormous burdens on New York businesses would result from requirements related to data retention, destruction, security, risk assessment, control system monitoring, etc., which would be imposed on businesses collecting biometric identifier information *"of any person."* It appears this is not limited to consumers or even people located in New York City, and also

[4] https://codelibrary.amlegal.com/codes/newyorkcity/latest/NYCadmin/0-0-0- 42626

[5] https://progresschamber.org/wp-content/uploads/2023/03/Who-Benefits-from-BIPA-Analysis-of-Cases-Under-IL-Biometrics-Law.pdf

includes employees. The result will be to discourage or even eliminate use of the technology in business operations such as for example, fingerprint timeclocks and cash register locks, biometrically secured building and door access control systems for workers, or biometrically secured driver authentication for ride-share services.

Safety/Security Applications: The proposal would also directly reduce the ability of businesses to continue to address the crisis of organized retail crime, which remains above pre-pandemic levels. According to NYPD data retail theft is down about 15% from last year.

We know that retailers across the city have embraced biometrically enabled security systems, as a key technology tool for fighting organized retail crime. There are many examples of the types of daily success achieved in preventing theft as well as violence against employees using these systems that leverage facial recognition technology,[6] and most often this involves de-escalation versus calls to authorities.

For example, when a repeat offender enters a store, typically a manager receives an alert and staff approach the individual with the goal of offering excellent customer service, rather than apprehending them. This often results in their departure from the store. This type of process was enough to help one retailer stop a shocking 90 percent of their repeat offenders.[7] Of course, a rigorous process must accompany such applications that strictly govern the conditions for enrollment of images, what personnel have access to a system, appropriate staff responses to an alert, adequate personnel training and other elements. The public is understandably becoming more concerned about safety in stores, and our independently conducted polling shows that 70% of Americans are supportive of using facial recognition software in improve safety and security in the workplace.[8]

We should remember that retail crime is often violent crime, it's not just "shoplifting." In just the first half of 2025, over 300 customers, employees, and security personnel were actually killed by criminals in retail settings, up 25% from 2025.[9] And the human cost extends far beyond these victims, as revenue generated from organized retail theft fuels drug smuggling, human trafficking, and other criminal enterprises and the violence that comes with it.

Nevertheless, the proposed Int. 213 would outright ban use of these critical technology tools, despite the benefits and the fact that the City's existing law already regulates the use of such systems.

Prohibiting Tenant Choice to Use Biometric Entry Options for Convenient, Secure Building Access

Similar to the impact of Int. 213 on commercial and consumer applications, Int. 428 would ban opt-in, voluntary uses of biometric technology, denying residents the choice to have more secure and convenient access to their buildings. Used ubiquitously throughout New York City, modern electronic access control systems are essential to keeping building occupants safe and secure. Data generated and used in such systems, including where this includes biometric information, is already regulated under New York City's Tenant Data Privacy Law which specifies that user consent is required.[10]

---

[6] https://lossprevention media.com/face-matching-leads-to-big-wins-for-retailers/

[7] Ibid.

[8] https://www.securityindustry.org/report/u-s-public-opinion-research-on-the-support-of-facial-recognition/

[9] https://d-ddaily.com/archivesdaily/2025-Mid-Year-Fatalities-Report.htm

[10] https://www.nyc.gov/site/hpd/services-and-information/tenant-data-privacy-law.page

Rather than regulating, this measure would ban biometrically enabled functions as part of these systems. One direct impact for will be barring use of increasingly popular "virtual" or "remote" doorman and concierge systems providing automatic tenant access at main entrances to residential buildings. Under these systems, those that choose to pre-enroll are automatically verified through the camera at the door, which then opens for them. For those not enrolled, the system reverts to the manual process where someone who wished to enter pushes a button and is connected to an operator who does the verification that they are tenant, authorized guest, delivery person, etc.

Biometric technologies offer faster and higher-assurance authentication for the user while reducing the transfer or exposure of information more vulnerable to exploitation (pin codes, etc) and addressing the risk of keys, cards or fobs being lost, stolen or misused. The security of a person's home is paramount. But people lose fobs and keys, especially their children coming home from school when the parents are still at work. Having another means that a person always has with them to get into a safe, secure space should be what the Council is concerned with. Should there be user consent and reasonable limitations? Yes. But an outright ban stops families from knowing that their loved one's have a way to get into their home when the inevitable happens — someone misplaces their keys or fob.

Enactment of this proposal would preclude residents from such options to use more secure, convenient and technologically advanced methods of authentication and access. Importantly, these having these options are in fact among benefits guaranteed to tenants in many existing rental agreements.

Breaking Down Biometric Myths

We have found concerns about biometric technologies are often driven by common misconceptions about the security of data created by these systems, based largely on Hollywood portrayals and inaccurate media narratives.

Data created and matched by facial recogntion software is actually more secure and far less susceptible to compromise or abuse than other types of personal information – a fact that should inform any discussion around the potential privacy implications. This software generates and uses abstract numerical representations made by deep-learning models, not our actual physical features. The data is created and readable only within the specific proprietary software and system used, which is "matched" based on the mathematical similarity between "saved" and comparison information within that system.

This data is both irreversible (cannot be reverse engineered to reveal the image or feature measured), and unusable by third parties or within other systems and databases. This "natural cryptography" makes it far less vulnerable than information like social security numbers, PINs and passwords, which are easily exploited by identity thieves and cyber-attackers.

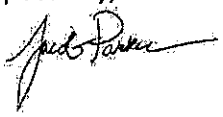
You may have heard something like "passwords can be reset, facial recognition data can't." Yet this is false. Even in the unlikely event of a database breach involving biometric data (which is unusable outside it) operators can swiftly respond by simply updating to a new software version or encrypting the data with a new key. Data utilized by facial recogntion software is also infinitely changeable for the same individual, in that it will be represented slightly differently each time it is created by the software (due to varying camera positions or photography conditions for example), for enrollment or comparison. This data can easily be "reset" as needed.

Finally, there is the long-outdated notion that facial recognition technology is plagued by race, gender, and age bias. While early versions struggled to perform consistently across various demographic factors, modern technologies exhibit minimal "bias." U.S. government testing data, which is the most reliable information available, shows that the leading technologies used in products today are well over 99% accurate overall and more than 97.5% accurate across more than 70 different demographic variables.[11]

Conclusion

We support legislation, policies and best practices that help ensure responsible and effective use of biometric technologies and the societal benefits that flow. We believe such measured approaches should be utilized to address specific concerns, not categorical bans on technology. For all the reasons above we urge the Technology Committee not to approve these measures. We also stand ready to provide any additional information or expertise needed as you consider these important issues.

Respectfully,



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

[11] https://www.securityindustry.org/2022/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/

THE LEGAL AID SOCIETY CRIMINAL DEFENSE

TESTIMONY

The Council of the City of New York
Committee on Technology

An Oversight Hearing on Facial Recognition Technology and the Collection of Biometric Data

March 2, 2026

The Legal Aid Society
Criminal Defense Practice
49 Thomas Street
New York, NY 10013

By: Laura Moraff
Digital Forensics Unit
Staff Attorney
(929) 536-1637
LMoraff@legal-aid.org

Contents

Good morning. I am Laura Moraff, a Staff Attorney in The Legal Aid Society's Digital Forensics Unit, which is a specialized unit that works on electronic surveillance and digital evidence issues in all five boroughs. I thank the Committee for the opportunity to provide testimony about facial recognition technology and the collection of biometric data, and urge the Council to pass Intro 213 and Intro 428 (with the amendments discussed herein), as well as a bill banning New York City government entities from using biometric recognition technologies.

I. ORGANIZATIONAL INFORMATION

Since 1876, The Legal Aid Society (LAS) has provided free legal services to New York City residents who are unable to afford private counsel. Annually, through our criminal, civil and juvenile offices, our staff handles over 180,000 matters for low-income families and individuals. By contract with the city, LAS serves as the primary defender of indigent people prosecuted in the state court system.

In 2013, LAS created the Digital Forensics Unit to serve and support LAS attorneys and investigators in cases involving digital evidence and electronic surveillance issues. Through investigation, research, and FOIL requests, the Unit aims to maintain an up-to-date understanding of the surveillance technologies and practices used in New York City, so that we can better serve our current and future clients in criminal, juvenile, and civil cases. The Digital Forensics Unit's attorneys and analysts also work to educate clients, attorneys, judges, and the public on digital forensics issues, and advocate for legislation to protect the privacy of all New Yorkers, including the most vulnerable among us.

II. BACKGROUND ON BIOMETRIC RECOGNITION TECHNOLOGY

Biometric recognition technologies purport to identify individuals based on their bodily

characteristics. For example, facial recognition technology attempts to identify individuals by comparing their face to faces in an existing database. The technology's ability to accurately identify individuals depends on how it was trained. Because many facial recognition technologies are primarily trained on middle-aged white men with no facial anomalies, the technologies are less accurate at identifying people of color, women, children, elderly individuals, and people with facial disfigurements or other conditions affecting their facial appearance.[1] Facial recognition algorithms may also fail to correctly match a person to their photo when the person has changed their hairstyle, applied makeup, or aged,[2] or where their photo was underexposed—which occurs more frequently for dark-skinned people.[3] And even as facial recognition tools' reported accuracy rates improve, they continue to underperform in real-world settings where faces are partially obscured, moving, or in less-than-ideal lighting conditions.[4]

Disparities exist in the reliability of other forms of biometric recognition tools as well. Like facial recognition, iris recognition[5] and voice recognition[6] are less reliable when used on female subjects. Voice recognition may also be less reliable for people with accents

---

[1] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance* at 56, The National Academies Press (2024), https://doi.org/10.17226/27397; Joy Buolamwini, *Unmasking the Bias in Facial Recognition Algorithms*, MIT Sloan School of Management (Dec. 13, 2023), https://mitsloan.mit.edu/ideas-made-to-matter/unmasking-bias-facial-recognition-algorithms; Matt Burgess, *When Face Recognition Doesn't Know Your Face Is a Face*, Wired (Oct. 15, 2025), https://www.wired.com/story/when-face-recognition-doesnt-know-your-face-is-a-face/.

[2] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance* at 57–58, The National Academies Press (2024), https://doi.org/10.17226/27397;

[3] *Id.* at 58.

[4] Teo Canmetin et al., *Why We Shouldn't Trust Facial Recognition's Glowing Test Scores*, Tech Policy Press (Aug. 18, 2025), https://www.techpolicy.press/why-we-shouldnt-trust-facial-recognitions-glowing-test-scores/.

[5] Meiling Fang et al., *Demographic Bias in Presentation Attack Detection of Iris Recognition Systems* at 1, 28th European Signal Processing Conference (2020), https://www.researchgate.net/publication/348733849_Demographic_Bias_in_Presentation_Attack_Detection_of_Iris_Recognition_Systems.

[6] M. Estevez and L. Ferrer, *Study on the Fairness of Speaker Verification Systems Across Accent and Gender Groups*, at 1, IEEE International Conference on Acoustics, Speech and Signal Processing, Rhodes Island, Greece, 2023, doi: 10.1109/ICASSP49357.2023.10095150.

underrepresented in the system's training data.[7] And speech features can change with age, sickness, exhaustion, and tension, making identity verification based on voice prints challenging and potentially inaccurate.[8]

The flaws and biases in these biometric recognition systems are well known and predictably lead to unjustified exclusion and discrimination. But even as the tools advance and become more accurate, they still pose a major threat to our freedoms. Biometric recognition technologies can track individuals throughout their daily lives—as they attend protests, seek reproductive healthcare, and visit houses of worship. It is no wonder that these tools are so attractive to authoritarian governments.[9] Russia has used facial recognition technology to identify and detain protestors.[10] China has used facial recognition technology to identify Uighurs based on their physical attributes.[11] Hungary banned pride events and vowed to use facial recognition technology to identify those who attempted to attend.[12] As our own federal government ramps up its biometric surveillance efforts,[13] it is more crucial than ever that local

---

[7] *Id.*

[8] Khushboo Jha et al. *Analysis of Human Voice for Speaker Recognition: Concepts and Advancement* at 13, J. Electr. Syst. 20.1s (2024), https://www.researchgate.net/profile/Khushboo-Jha-2/publication/379678575_Analysis_of_Human_Voice_for_Speaker_Recognition_Concepts_and_Advancement/links/6659d32e0b0d28457475fd25/Analysis-of-Human-Voice-for-Speaker-Recognition-Concepts-and-Advancement.pdf

[9] *See, e.g.*, Dia Kayyali, *The High Stakes of Biometric Surveillance*, Tech Policy Press (Jun. 23, 2025), https://www.techpolicy.press/the-high-stakes-of-biometric-surveillance/.

[10] Lena Masri, *Facial Recognition Is Helping Putin Curb Dissent with the Aid of U.S. Tech*, Reuters (Mar. 28, 2023), https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/.

[11] Paul Mozur, *One Month, 500,000 Face Scans: How Chine Is Using A.I. to Profile a Minority*, New York Times (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html?searchResultPosition=3; Alfred Ng, *How China Uses Facial Recognition to Control Human Behavior*, CNET (Aug. 11, 2020), https://www.cnet.com/news/politics/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/.

[12] Ashifa Kassam, *Hungary Bans Pride Events and Plans to Use Facial Recognition to Target Attenders*, The Guardian (Mar. 18, 2025), https://www.theguardian.com/world/2025/mar/18/hungary-bans-pride-events-and-plans-to-use-facial-recognition-to-target-attenders.

[13] *See, e.g.*, Sheera Frenkel & Aaron Krolik, *How ICE Already Knows Who Minneapolis Protesters Are*, New York Times (Jan. 30, 2026), https://www.nytimes.com/2026/01/30/technology/tech-ice-facial-recognition-palantir.html; Joseph Cox, *Ice Spends Millions on Clearview AI Facial Recognition to Find People 'Assaulting' Officers*, 404 Media (Sep. 8, 2025), https://www.404media.co/ice-spends-millions-on-clearview-ai-face-recognition-to-find-people-assaulting-officers/; Joseph Cox, *DHS Gives Local Cops a Facial Recognition App to Find Immigrants*, 404 Media (Nov. 4, 2025), https://www.404media.co/cbp-quietly-launches-face-scanning-app-for-local-cops-to-do-

governments step in to protect their populations' biometric data and freedom.

Biometric data is often impossible to change, which means that once it is collected, any security breach can jeopardize individuals' safety and security forever.[14] When a hacker gets ahold of a person's credit card number or password, for example, the person can create new ones and secure their information for the future. When a hacker gets ahold of a person's biometric data, however, the person is at constant risk of identity theft for the rest of their life, and accounts "secured" using biometrics are no longer secure.[15]

The best way to secure such information is to refrain from collecting it in the first place. Luckily, the purposes for which biometric information is collected can easily be served through other means. Providers of public accommodation can protect the security of their stores using traditional alarms for stolen goods. Landlords can grant and deny entry to residential buildings using physical keys. And law enforcement can locate and identify individuals through traditional investigative techniques that are based on facts and reason as opposed to race and algorithmic bias.

By restricting the collection and use of biometric data in New York City, the Council can preserve New Yorkers' right to live freely and autonomously and protect New Yorkers' biometric information from exploitation. The Legal Aid Society urges the Council to ban the use of biometric recognition technology by providers of public accommodations, residential buildings, and the government.

---

immigration-enforcement/; Craig McKee, *DHS Proposal Would Expand Biometric Data Collection in Immigration Cases, Including for Some U.S. Citizens*, ABC 15 (Jan. 2, 2026), https://www.abc15.com/news/national/dhs-proposal-would-expand-biometric-data-collection-in-immigration-cases-including-for-some-u-s-citizens.

[14] *See* Mohamed Lazzouni, *What Happens If Biometric Data Is Breached (And How to Prevent It)*, Forbes (Apr. 25, 2025), https://www.forbes.com/councils/forbestechcouncil/2025/04/25/what-happens-if-biometric-data-is-breached-and-how-to-prevent-it/.

[15] Taryn Plumb, *Face Off: Attackers Are Stealing Biometrics to Access Victim's Bank Accounts*, Venture Beat (Feb. 21, 2024), https://venturebeat.com/security/face-off-attackers-are-stealing-biometrics-to-access-victims-bank-accounts.

III. BIOMETRIC SURVEILLANCE IN PLACES OF PUBLIC ACCOMMODATION (INTRO 213)

New Yorkers rely on places of public accommodation—including grocery stores, restaurants, entertainment venues, pharmacies, hospitals, shops, and any other provider of goods, services, facilities, accommodations, advantages or privileges of any kind—to get through our daily lives. When we go to a store to pick up bread, diapers, or medicine, we should not have to worry that we will be watched, followed, or even kicked out because a technology with known inaccuracies and biases has flagged us as suspicious. And meeting our basic needs shouldn't come at the cost of giving up our privacy in our faceprints, voiceprints, and other largely unchangeable biometric information.

Yet across this City, shoppers, patients, concert-goers, and sports fans are being surveilled and discriminated against by corporations using biometric recognition technology. Gothamist recently published an article about Wegmans collecting biometric data, including faceprints, eye scans, and voiceprints, from everyone who enters their stores in New York City.[16] Other retailers in NYC, including Macy's and Fairway, also collect customers' biometric information.[17]

Examples abound of the harms caused by this type of biometric surveillance—both when it fails to correctly identify people and when it succeeds. In 2023, Rite Aid was prohibited from using facial recognition technology to surveil its customers after the Federal Trade Commission found that Rite Aid's facial recognition technology was falsely flagging people—disproportionately women and people of color—as potential shoplifters, leading to increased

[16] Liam Quigley, *NYC Wegmans Is Storing Biometric Data on Shoppers' Eyes, Voices and Faces*, Gothamist (Jan. 3, 2026), https://gothamist.com/news/nyc-wegmans-is-storing-biometric-data-on-shoppers-eyes-voices-and-faces.
[17] Paige Oamek & Andrew Giambrone, *Not Just Wegmans: More NYC Retailers Using Facial Recognition As Tech Outpaces Law*, Gothamist (Jan. 12, 2026), https://gothamist.com/news/not-just-wegmans-more-nyc-retailers-using-facial-recognition-as-tech-outpaces-law.

surveillance and accusations against them.[18] Disparities persist in the facial recognition technology's reliability across race and gender lines, meaning the consequences of its errors fall disproportionally on Black, brown, and female New Yorkers.

When facial recognition technology *does* accurately identify people, it allows corporations to deny goods and services to anyone they dislike for any reason. For example, Madison Square Garden Entertainment Corporation ("MSG") uses facial recognition technology in its entertainment venues to identify and keep out attorneys who work at law firms that litigate against the Corporation.[19] In 2022, a mother who was trying to watch the Rockettes show with her daughter and her daughter's Girl Scout troop was prohibited from entering Radio City Musical Hall (owned by MSG) because she worked at a law firm that was involved in personal injury litigation against one of MSG's restaurants (though she, herself, had not worked on cases against MSG).[20] MSG also used facial recognition technology to identify and ban the designer of a T-shirt making fun of MSG CEO James Dolan.[21]

Biometric recognition technology can also facilitate price gouging. As the technology identifies and tracks people throughout a store, it can inform inferences about how much an individual would be willing to pay for a given item—based on other known information about the individual and/or data on how long they linger in a particular aisle or look at a particular

---

[18] Press Release, Federal Trade Commission, *Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards* (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without; Shaun Harper, *Rite Aid Facial Recognition Lawsuit Shows AI Risks of Shopping While Black*, Forbes (Dec. 21, 2023), https://www.forbes.com/sites/shaunharper/2023/12/21/shopping-while-black-in-the-era-of-ai-lessons-from-a-federal-case-against-rite-aid/.

[19] Devin Gordon, *When Knicks Fans Are Banned from Madison Square Garden, Is There Any Coming Back?*, ESPN (Aug. 13, 2025), https://www.espn.com/nba/story/_/id/45949758/new-york-knicks-msg-banned-list-james-dolan.

[20] Julianne McShane, *Girl Scout Mom Kicked Out of Radio City Barred from Seeing Rockettes After Facial Recognition Tech Identified Her*, NBC News (Dec. 21, 2022), https://www.nbcnews.com/news/us-news/girl-scout-mom-kicked-radio-city-barred-seeing-rockettes-facial-recogn-rcna62606.

[21] Mia Sato, *Madison Square Garden's surveillance system banned this fan over his T-shirt design*, The Verge (Mar. 28, 2025), https://www.theverge.com/news/637228/madison-square-garden-james-dolan-facial-recognition-fan-ban.

product.[22] A grocery store might use biometric recognition technology to identify those who would pay an extra dollar for bread or eggs, and then charge them that increased price.[23]

In addition to facilitating discrimination, the implementation of facial recognition technology in places of public accommodation chills vulnerable populations from accessing those places because the data might be weaponized against them. Unless the Council acts, customers' biometric information may be shared with local or federal law enforcement, and with data brokers, who in turn sell it to others.[24]

This is particularly concerning to New York's immigrant communities, as Immigration and Customs Enforcement (ICE) routinely purchases surveillance data from private companies.[25] Across the City, immigrants are afraid to go grocery shopping, dine out, or receive medical care, because doing so might lead to an encounter with ICE.[26] The City of New York should be able to

---

[22] Kristin Schwab, *At Grocery Stores, Shopping with a Side of Biometric Surveillance*, Marketplace (Jan. 8, 2026), https://www.marketplace.org/story/2026/01/08/how-grocery-stores-use-surveillance-to-track-shoppers.

[23] *See* Alison Kuznitz, *Lawmakers Seek Ban on Grocery Store Price Adjustments, Targeted Ads Based on Biometric Data*, Worcester Business Journal (Aug. 19, 2025), https://wbjournal.com/article/lawmakers-seek-ban-on-grocery-store-price-adjustments-targeted-ads-based-on-biometric-data/; Mayu Tobin-Miyaji, *Kroger's Surveillance Pricing Harms Consumers and Raises Prices, With or Without Facial Recognition*, Electronic Privacy Information Center (Feb. 14, 2025), https://epic.org/krogers-surveillance-pricing-harms-consumers-and-raises-prices-with-or-without-facial-recognition/.

[24] *See, e.g.*, Dell Cameron, *Surveillance and ICE Are Driving Patients Away from Medical Care, Report Warns*, Wired (Jan. 21, 2026), https://www.wired.com/story/surveillance-and-ice-are-driving-patients-away-from-medical-care-report-warns/; Joseph Cox, *Airlines Don't Want You to Know They Sold Your Flight Data to DHS*, 404 Media (Jun. 10, 2025), https://www.404media.co/airlines-dont-want-you-to-know-they-sold-your-flight-data-to-dhs/; Devan Burris, *How Grocery Stores Are Becoming Data Brokers*, CNBC (Dec. 10, 2023), https://www.cnbc.com/2023/12/10/how-grocery-stores-are-becoming-data-brokers.html?msockid=060681ce093b6e1c374c947c08ef6f5d.

[25] Nina Wang, Allison McDonald, Daniel Bateyko & Emily Tucker, *American Dragnet: Data-Driven Deportation in the 21st Century*, Center on Privacy & Technology at Georgetown Law (May 10, 2022), https://www.americandragnet.org.

[26] Rong Xiaoqing, *It's Quieter Now. People Are Afraid.*, New York Times (Feb. 7. 2026), https://www.nytimes.com/2026/02/07/opinion/queens-raids-immigration.html; Jennifer Bisram, *Some Haitian Immigrants in NYC Still Living in Fear Despite TPS Reprieve*, CBS News (Feb. 4, 2026), https://www.cbsnews.com/newyork/news/nyc-haitian-immigrants-tps/; *Immigrants Report Rising Fear, Negative Economic and Health Impacts, and Changing Political Views During the First Year of President Trump's Second Term*, KFF (Nov. 18, 2025), https://www.kff.org/racial-equity-and-health-policy/immigrants-report-rising-fear-negative-economic-and-health-impacts-and-changing-political-views-during-the-first-year-of-president-trumps-second-term/; Daniel Parra, *Federal Crackdown Is Taking a Toll on Immigrant New Yorkers' Meantal Health, Officials & Advocates Say*, City Limits (Sep. 18, 2025), https://citylimits.org/federal-crackdown-is-taking-a-toll-on-immigrant-new-yorkers-mental-health-officials-advocates-say/; Emily Baumgaertner Nunn et al., *Migrants Are*

guarantee that leaving one's home does not mean relinquishing all privacy in one's biometric data to businesses—and eventually governments—that may use the data to expel them from the country.

Banning facial recognition in places of public accommodation is necessary to ensure New Yorkers are able to access essential businesses and entertainment venues without fear of being tracked or excluded. Enacting Intro 213 would help accomplish this goal by making it unlawful for a place of public accommodation to use any biometric recognition technology to identify a customer, Section 2(b), or to disclose, sell, or share biometric information with any third party, Section 2(c).

Where providers of public accommodations wish to collect biometric identifier information for other purposes, the bill requires that they obtain written consent from customers before collecting their biometric identifier information, Section 2(a), and permit customers to request that their biometric identifier information be erased, Section 2(f). The bill further ensures that those who withhold their written consent or request that their biometric identifier information be erased are not penalized by—for example—being denied goods or services or being charged different prices. Section 2(g).

Currently, places of entertainment, retail stores, and food and drink establishments that collect certain types of biometric identifier information are required to disclose that fact with a clear and conspicuous sign near all entrances. Intro 213 extends that requirement to all places or providers of public accommodation, meaning that all providers of goods, services, facilities, accommodations, advantages or privileges of any kind must adhere to this requirement—as well as the others in the bill.

Skipping Medical Care, Fearing ICE, Doctors Say, New York Times (May 8, 2025), https://www.nytimes.com/2025/05/08/health/migrants-health-care-trump.html.

The bill also contains a private right of action. Section 3. Private rights of action are critical, especially in privacy legislation, to ensure that rights under the law are not merely theoretical. The private right of action in this bill is appropriately robust when a provider of public accommodation uses biometric recognition technology to identify a customer and when a place of public accommodation discloses or otherwise profits from the transaction of biometric identifier information with any third party.

However, the current draft of the bill has a significantly weaker private right of action for situations where a place of public accommodation fails to disclose that they are collecting, retaining, converting, storing, sharing, or obtaining biometric identifier information from customers. In such situations, the bill requires that a person whose biometric identifier information was collected or shared without their knowledge provide written notice of their allegations to the place of public accommodation. Section 3. If the public accommodation cures the violation and states in writing that the violation has been cured and no further violations will occur, then the aggrieved customer cannot initiate action against the place of public accommodation. Section 3. **The bill should be amended to eliminate the notice requirement,** so that providers of public accommodations are incentivized to comply with the law at its onset, rather than wait to see if individuals or organizations will threaten legal action to force them to comply.

We urge the Council to pass Intro 213, with the amendments proposed above, to protect individual's privacy and control over their biometric identifier information and prevent places of public accommodation from using inaccurate and discriminatory systems to surveil and ban customers.

IV. BIOMETRIC SURVEILLANCE IN RESIDENTIAL BUILDINGS (INTRO 428)

Submitting to surveillance should not be a condition of going home. But across New York, landlords are compelling tenants to submit to biometric recognition systems before entering their apartments.

When landlords use biometric recognition technology to decide who is permitted to enter a building, tenants may be stuck outside until they figure out how to overcome the technology's error. As detailed in an op-ed by a Black woman residing in the Bronx who was stuck outside in the rain because her building's facial recognition system failed to identify her, such systems are not only inconvenient; they place residents in danger.[27] The systems may also struggle to identify residents on sunny or rainy days.[28]

As in the public accommodations context, biometric surveillance is just as harmful when it *can* identify tenants as when it cannot. Some landlords use facial recognition systems in an effort to catch minor lease violations—such as having overnight visitors for too many nights in a year—and evict tenants.[29] For example, a Massachusetts resident was served an eviction notice because the local housing authority surveilled her apartment and claimed that her ex-husband was living there without paying rent; the resident maintained that her ex-husband lived elsewhere but visited her to help out with child care.[30]

Some tech companies are even marketing biometric surveillance tools as means of raising

---

[27] Lyla Renwick-Archibold, *Op-Ed: Facial Recognition locked Me Out of my Own Apartment. NYS Must Ban it*, New York Amsterdam News (May 30, 2024), https://amsterdamnews.com/news/2024/05/30/op-ed-nys-must-ban-facial-recognition/

[28] Elizabeth Kim, *'We're Like Guinea Pigs': How An Affordable Lower East Side Complex Got Facial Recognition*, Gothamist (Sep. 8, 2019), https://gothamist.com/news/were-guinea-pigs-how-affordable-lower-east-side-complex-got-facial-recognition.

[29] Douglas MacMillan, *Eyes on the Poor: Cameras, Facial Recognition Watch Over Public Housing*, Washington Post (May 16, 2023), https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/.

[30] *Id.*

rents in New York City.[31] For example, Teman GateGuard advertises itself as an "AI doorman" to tenants, but it has been marketed to landlords as a means of recording minor lease violations in order to evict tenants and raise rents.[32] The company's founder even bragged in a 2018 LinkedIn post that his company had "EVICTED OVER 600 STABILIZED TENANTS in the last 2 years."[33] The post does not address the concerns of rent-stabilized tenants who prefer not to be constantly surveilled as they enter and exit their homes. [34]

The harms perpetuated by biometric recognition tools are easily avoidable in the residential context. The use of facial recognition or other biometric identification technology to grant and deny entry into residential buildings is entirely unnecessary, and far more dangerous than traditional physical keys.

For these reasons, The Legal Aid Society strongly supports Intro 428, which prohibits owners of residential buildings that house three or more families from using biometric recognition technology that identifies tenants or guests of tenants.

As discussed above, private rights of action are crucial to enforcing privacy rights. **We therefore urge the Council to amend the bill to add a private right of action allowing tenants and guests of tenants to hold landlords accountable when they violate the law.**

V. BIOMETRIC SURVEILLANCE BY THE GOVERNMENT

The Legal Aid Society is acutely aware of the ways in which government use of biometric recognition technology can prejudice our clients' rights and make all New Yorkers less

[31] Taylor Lorenz, *Landlords Are Using Facial Recognition to Raise Your Rent*, Patreon (Aug. 23, 2025), https://www.patreon.com/posts/landlords-are-to-137187579.
[32] Alec Bacon & Sean Mcdonald, *PropTech's Digital Pipeline to Prison*, Tech Policy Press (Jan. 29, 2025), https://www.techpolicy.press/proptechs-digital-pipeline-to-prison/.
[33] Nick Keppler, *Meet the Spy Tech Companies Helping Landlords Evict People*, Vice (Jan. 4, 2023), https://www.vice.com/en/article/meet-the-spy-tech-companies-helping-landlords-evict-people/.
[34] *See* Ari Teman, *5 Ways to Maximize Evictions (NYC Multifamily)*, LinkedIn (Nov. 9, 2018), https://www.linkedin.com/pulse/5-ways-maximize-evictions-nyc-multifamily-ari-teman/.

safe. For example, the New York City Police Department (NYPD) routinely uses facial recognition technology to attempt to identify criminal suspects and arrest people. The NYPD often runs facial recognition algorithms on still shots taken from bodega security cameras or other footage that is blurry, taken from odd angles, or otherwise unable to accurately portray a person's face. The NYPD sometimes alters the still shots to increase the likelihood that their facial recognition technology will identify a match—which only compounds the risk that the wrong person will be selected as the criminal suspect.[35] Such alterations can include modifications to hair, head coverings, or make-up.[36] Officers have even used photos of celebrities who they believe resemble a suspect to try to find a match using facial recognition technology.[37]

For our clients who have been wrongly arrested based on false facial recognition matches, the consequences cannot be overstated. On top of the physical and emotional trauma of being arrested—sometimes in front of their children or neighbors—they suffer extreme psychological distress and lose professional licenses, job opportunities, and standing in their communities. These consequences fall disproportionately on our Black clients, both because of the racial biases baked into facial recognition systems, and because surveillance cameras whose footage can be run through facial recognition algorithms are disproportionately concentrated in non-white neighborhoods.[38]

Most wrongful arrests based on facial recognition are never disclosed to the public. Our

---

[35] *See* 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.

[36] Jocelyn Strauber & Jeanene Barrett, *An Assessment of NYPD's Response to the POST Act* at 26 (Nov. 2022), https://www.nyc.gov/assets/doi/reports/pdf/2022/POSTActReport_Final_11032022.pdf.

[37] 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.

[38] *Inside the NYPD's Surveillance Machine*, Amnesty International, https://banthescan.amnesty.org/decode.

clients are often hesitant to talk to the press about the worst days of their lives, and sometimes we are unable to get the documentation we need to show exactly how and why the NYPD's facial recognition technology failed. But as law enforcement is increasingly relying on this unreliable and dangerous technology, the number of wrongful arrests is increasing, and some affected individuals are starting to come forward.[39]

In February of 2025, a woman reported to police that she had been flashed by a 5-foot-6 Amazon delivery worker. The NYPD obtained surveillance footage and used facial recognition technology to identify our client, Trevis Williams, as a possible match for the suspect. Mr. Williams is 8 inches taller and 70 pounds heavier than man described by the woman. And location data from his phone showed that he was 12 miles away from the alleged crime. But instead of investigating further, police went ahead and arrested Mr. Williams. Mr. Williams spent more than two days in jail because the NYPD used unreliable technology to supplant traditional police work.[40] During his time in jail, Mr. Williams feared the erroneous charges could place him on a sex offender registry, making it impossible for him to continue his counseling work with autistic adults or even pick up his 12-year-old son from school. He described feeling humiliated, terrified, and on the verge of panic attacks.[41]

In Detroit, Porcha Woodruff, an innocent Black woman, was wrongfully arrested and held in jail for 11 hours—while eight months pregnant—after being misidentified by facial

---

[39] *See, e.g.*, Maria Cramer & Kashmir Hill, *How the N.Y.P.D.'s Facial Recognition Tool Landed the Wrong Man in Jail*, New York Times (Aug. 26, 2025), https://www.nytimes.com/2025/08/26/nyregion/nypd-facial-recognition-dismissed-case.html; Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, New York Times (Aug. 6, 2023), https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html; Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*, Wired (Mar. 7, 2022), https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/; Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, New York Times (Dec. 29, 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[40] *See generally* Maria Cramer & Kashmir Hill, *How the N.Y.P.D.'s Facial Recognition Tool Landed the Wrong Man in Jail*, New York Times (Aug. 26, 2025), https://www.nytimes.com/2025/08/26/nyregion/nypd-facial-recognition-dismissed-case.html.

[41] *Id.*

recognition and falsely accused of robbery and carjacking.[42] Her time in jail caused serious medical complications, including contractions and sharp pain, requiring her to be hospitalized immediately upon release.

Three Black fathers, two in Detroit and one in New Jersey, were wrongfully arrested and jailed following faulty facial recognition matches, and suffered devastating, lasting consequences.[43] Another Black man was wrongfully arrested in Georgia for a crime committed in Louisiana and spent six days in jail, despite the fact that had never been to Louisiana.[44] And just last week, The Guardian reported that a south Asian software engineer in the UK was arrested because facial recognition technology erroneously matched him with footage of a suspect who was noticeably younger and had visibly different features.[45]

Government entities have also used biometric recognition technology to surveil, identify, and target protestors, chilling free speech and punishing individuals for exercising their constitutional rights.[46] In 2020, the NYPD reportedly used facial recognition to target Derrick Ingram after he participated in a protest against police brutality. [47] Police later surrounded Mr. Ingram's apartment with more than 50 officers as part of a retaliatory raid.[48] In 2024, the New York City Fire Department used facial recognition technology to identify Zuhdi Ahmed, a 21-

---

[42] Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, New York Times (Aug. 6, 2023), https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.
[43] Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*, Wired (Mar. 7, 2022), https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/.
[44] Sudhin Thanawala, *Facial Recognition Technology Jailed a Man for Days. His Lawsuit Joins Others from Black Plaintiffs*, AP News (Sep. 25, 2023), https://apnews.com/article/mistaken-arrests-facial-recognition-technology-lawsuits-b613161c56472459df683f54320d08a7.
[45] Robert Booth & Mark Wilding, *Facial Recognition Error Prompts Police to Arrest Asian Man for Burglary 100 Miles Away*, The Guardian (Feb. 25, 2026), https://www.theguardian.com/technology/2026/feb/25/facial-recognition-error-prompts-police-to-arrest-asian-man-for-burglary-100-miles-away.
[46] 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.
[47] *Id.*
[48] *Id.*

year-old protester, so that the NYPD could arrest him.[49] After a year of litigation, his charges were ultimately dismissed by the court.[50]

The Council should not wait for more New Yorkers to be wrongfully surveilled or arrested before banning the government from using this technology. **The Legal Aid Society urges the council to introduce and pass a bill prohibiting law enforcement and other government entities from using biometric recognition technology.**

VI. CONCLUSION

The Legal Aid Society encourages the City Council to enact Intro 213 and Intro 428 with the amendments described herein, and to introduce a bill to prohibit the government from using biometric recognition technology. We thank the Council for its attention to these important matters.

[49] Samantha Maldonado, *NYPD Bypassed Facial Recognition Ban to ID Pro-Palestinian Student Protester*, The City (Jul. 18, 2025), https://www.thecity.nyc/2025/07/18/nypd-fdny-clearview-ai-ban-columbia-palestinian-protest/.
[50] *People v. Zuhdi A.*, 86 Misc. 3d 1227(A) (N.Y. Co. Crim. Ct. 2025).

THE CENTER ON RACE INEQUALITY & THE LAW
NYU SCHOOL OF LAW

Center on Race, Inequality, and the Law
New York University School of Law
139 MacDougal Street, Fourth Floor
New York, NY 10012

TESTIMONY OF NINA LOSHKAJIAN
TECHNOLOGY & RACIAL JUSTICE COLLABORATIVE FELLOW

ON BEHALF OF THE CENTER ON RACE, INEQUALITY, AND THE LAW AT NEW YORK UNIVERSITY SCHOOL OF LAW

BEFORE THE NEW YORK CITY COUNCIL COMMITTEE ON TECHNOLOGY

REGARDING THE OVERSIGHT OF FACIAL RECOGNITION TECHNOLOGY AND THE COLLECTION OF BIOMETRIC DATA

IN SUPPORT OF INTROS. 213 AND 428

MARCH 2, 2026

Dear Chair De La Rosa and Committee Members,

Thank you for convening this important oversight hearing and for the opportunity to submit testimony. The Center on Race, Inequality, and the Law at New York University School of Law (the "Center") confronts and upends the array of American laws, policies, and practices that lead to racial oppression and injustice. By illuminating the history and impact of racism on law and society, we are able to find solutions to the injustice it causes and take action to advance freedom and fairness, for everyone.

The Center strongly urges the passage of Intros. 213 and 428, which would protect New Yorkers from discriminatory surveillance by banning the use of biometric recognition technology in places of public accommodations and residential settings, respectively. Given the threat of ongoing algorithmic discrimination to communities historically impacted by systemic bias, New York City officials must ban the use of facial recognition technology in the most intimate of places—our homes—and in businesses like grocery stores that we all rely on for essential goods and services.

I. The Dangers of Biometric Surveillance

Facial recognition technology has bias baked in, with systems trained on datasets in which faces of color are underrepresented, leading to a higher likelihood that Black and brown New Yorkers will be misidentified and subjected to harmful consequences.

The issue of bias in facial recognition technology has been evident since the publication in 2018 of Joy Buolamwini and Timnit Gebru's seminal study, which found that commercial systems misidentified 34.7% of darker-skinned women and just 0.8% of light-skinned men.[1] Subsequent research, including a 2019 National Institute of Standards and Technology report, confirmed this algorithmic bias, finding that Black and Asian faces are between 10 and 100 times likelier to be misidentified than white male faces.[2] The vast majority of known wrongful arrests due to facial recognition mismatches have been of Black men and women.[3]

---

[1] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROCEEDINGS OF MACHINE LEARNING RESEARCH 1, 10 (2018), available at https://proceedings.mlr.press/v81/buolamwini18a.html.

[2] Sophie Bushwick, *How NIST Tested Facial Recognition Algorithms for Racial Bias*, SCIENTIFIC AMERICAN, Dec. 27, 2019, https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias; *see also* Mei Wang & Weihong Deng, *Deep Face Recognition: A Survey*, 215 NEUROCOMPUTING 429 (March 14, 2021), https://doi.org/10.1016/j.neucom.2020.10.081.

[3] Kashmir Hill & Ryan Mac, '*Thousands of Dollars for Something I Didn't Do*,' N.Y. TIMES, March 31, 2023, https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html; Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, N.Y. TIMES, Aug. 6, 2023, https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html; Maria Cramer & Kashmir Hill, *How the N.Y.P.D.'s Facial Recognition Tool Landed the Wrong Man in Jail*, N.Y. TIMES, Aug. 26, 2025, https://www.nytimes.com/2025/08/26/nyregion/nypd-facial-recognition-dismissed-case.html.

As other emerging methods of biometric recognition technology are increasingly being deployed in dangerous ways, it is crucial that Intros. 213 and 428 go beyond addressing solely the use of facial recognition technology and also tackle the issue of biometric surveillance broadly. Methods relying on fingerprints, DNA, gait, voice, or other unique characteristics have demonstrated similar shortcomings in preventing the replication of bias and producing false positives. A Stanford study of leading speech recognition tools found that, due to the lack of linguistic diversity in the datasets these tools were trained on, Black speakers were misunderstood twice as often as white speakers when saying the same words.[4] These bills anticipate future harmful applications of technology in order to establish meaningful, lasting safeguards in our city.

II. Intro. 213 - Public Accommodations Ban

New Yorkers deserve the ability to partake in everyday life—from a simple trip to the grocery store[5] to a night out at a concert[6]—without being subjected to intrusive and discriminatory surveillance. Intro. 213 is urgently needed to protect our community members from being tracked and wrongfully harassed. The bill would prohibit any place or provider of public accommodation from using any biometric recognition technology to verify or identify a customer or to bar entry to customers.

Grocery stores across the city, from Fairway[7] to Wegmans,[8] are subjecting customers to biometric recognition technology as a condition of entry. After recent media scrutiny, Wegmans released a statement explaining that it uses biometrics to identify "persons of interest... determined by our asset protection team based on incidents occurring on our property," and also based on, concerningly, "information from law enforcement."[9] This reference to collaborating with police, especially in such vague terms, should be a huge red flag. Advocates have raised concerns that

---

[4] Allison Koenecke, Andrew Nam, Emily Lake, Joe Nudell, Minnie Quartey, Zion Mengesha, Connor Toups, John R. Rickford, Dan Jurafsky, & Sharad Goel, *Racial Disparities in Automated Speech Recognition*, 14 Proc. Natl. Acad. Sci. U.S.A. 117, 7684–89 (March 23, 2020), https://doi.org/10.1073/pnas.1915768117; *see also* Stanford Computational Policy Lab, *The Race Gap in Speech Recognition Technology*, https://fairspeech.stanford.edu (last visited Feb. 26, 2026).

[5] Wegmans Food Markets, Inc., *Wegmans Statement on Facial Recognition Technology*, Wegmans Newsroom, https://www.wegmans.com/news-media/press-releases/wegmans-statement-on-facial-recognition-technology (last visited Feb. 26, 2026).

[6] Kashmir Hill & Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, N.Y. TIMES, Dec. 22, 2022, https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html.

[7] Lynda Baquero, *Your NYC Supermarket May Know Your Face Better Than You Think*, NBC NEW YORK, March 16, 2023, https://www.nbcnewyork.com/news/local/nyc-supermarket-uses-face-recognition-software-but-why-and-wheres-the-info-going/4157198.

[8] Liam Quigley, *NYC Wegmans Is Storing Biometric Data on Shoppers' Eyes, Voices and Faces*, GOTHAMIST, Jan. 3, 2026, https://gothamist.com/news/nyc-wegmans-is-storing-biometric-data-on-shoppers-eyes-voices-and-faces

[9] Wegmans Food Markets, Inc., *Wegmans Statement on Facial Recognition Technology*, Wegmans Newsroom, https://www.wegmans.com/news-media/press-releases/wegmans-statement-on-facial-recognition-technology (last visited Feb. 26, 2026).

Wegmans or other retailers could be using the tech to assist federal immigration agents.[10] As a sanctuary city, we cannot allow for this possibility to materialize in the wrongful detention of undocumented New Yorkers. Passing Intro. 213 is necessary to protect our immigrant neighbors.

Some of New York's most iconic entertainment venues are also using invasive biometric recognition technology, forcing music and sports fans to hand over their personal data or forego meaningful experiences with their friends and family. CitiField has employed a facial recognition ticketing system, in partnership with Wicket, since 2022.[11] Particularly alarming is the way in which James Dolan, owner of Madison Square Garden Entertainment Corporation, chose to deploy the tech at their venues, weaponizing it to bar ticketholders affiliated with law firms involved in ongoing lawsuits against the company.[12] New Yorkers are currently subject to the ridiculous and vengeful whims of business owners and will continue to be at risk of wrongful exclusion and harassment until the Council passes this important piece of legislation.

The Council should also be skeptical of allowing businesses to collect data of such a sensitive nature as biometric identifier information. In 2023, the Federal Trade Commission ("FTC") barred Rite Aid from using facial recognition technology for five years because the company failed to implement safeguards to protect its customers.[13] The FTC complaint against Rite Aid highlighted in particular that the company "failed to consider whether its policies related to the selection of certain stores to use facial recognition technology, including prioritizing what it called 'urban' areas and stores along public transportation routes, would disproportionately impact certain populations, including racial or ethnic minority populations."[14] This led to facial recognition technology being deployed disproportionately in stores located in communities of color.[15] The Rite Aid case confirms the risks of allowing stores to deploy biometric surveillance, from racial bias to infringing on customers' privacy, and serves as an important cautionary tale.

---

[10] Jay Stanley, *Retailers Secretively Using Face Recognition to Spot 'Persons of Interest'—Including for the Government*, ACLU FREE FUTURE NEWSLETTER, Jan. 20, 2026, https://www.aclu.org/news/privacy-technology/retailers-secretively-using-face-recognition.

[11] 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; *see also* Dean Balsamini, *Mets Used Facial Recognition to Profit on Unsuspecting Citi Field Fans: Suit*, N.Y. POST, Oct. 12, 2024, https://nypost.com/2024/10/12/us-news/mets-used-facial-recognition-to-profit-on-unsuspecting-citi-field-fans-suit.

[12] Kashmir Hill & Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, N.Y. TIMES, Dec. 22, 2022, https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html.

[13] https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without

[14] Compl. ¶ 41, *F.T.C. v. Rite Aid Corp. et. al*, No. 2:23-CV-05023 (E.D. Pa. Dec. 19, 2023) https://www.ftc.gov/system/files/ftc_gov/pdf/2023190_riteaid_complaint_filed.pdf.

[15] *Id.* ¶ 42. ("In fact, although approximately 80 percent of Rite Aid stores are located in plurality-White (i.e., where White people are the single largest group by race or ethnicity) areas, about 60 percent of Rite Aid stores that used facial recognition technology were located in plurality non-White areas. As a result, store patrons in plurality-Black, plurality-Asian, and plurality-Latino areas were more likely to be subjected to and surveilled by Rite Aid's facial recognition technology.")

The Council should heed the many warning signs about the dangers of biometric surveillance in city businesses and pass Intro. 213.

III. Intro 428 – Residential Ban

Our homes should be where we all enjoy the fullest freedom of movement and highest levels of privacy, not testing grounds for biometric surveillance technologies. Intro. 428 would protect New Yorkers in residential settings, prohibiting owners of multiple dwellings from installing, activating or using any biometric recognition technology that identifies tenants or the guest of a tenant.

Tenants of color and their guests are at higher risk of being locked out of their homes due to the racial bias of facial recognition technology.[16] This will result in people being stranded outside in inclement weather until the system recognizes them, and might even prompt harmful and unwarranted law enforcement response where someone is wrongfully accused of trying to break into their own home. [17]

Landlords have already started to weaponize this tech in cruel ways, including to evict tenants for minor rent violations or to justify rent increases.[18] In one case, a single mother, Tania Acabou, was evicted from public housing because the technology flagged her for violating a guest policy, only because her ex-husband routinely came over to watch their child while she attended night classes.[19] Mrs. Acabou's experience reveals the inevitable consequence of allowing such technology to be used: low-income, communities of color suffer the worst harms.[20] Biometric recognition technology also negatively affects tenants' personal relationships, subjecting their family and friends to unwarranted surveillance.

There are also concerns around exposing our immigrant neighbors to ICE—as landlords could retaliate against their tenants by handing over the data their systems collect to federal authorities. Such concerns are not strictly hypothetical, and allowing the collection of the most sensitive information—in the form of biometric identifiers—exposes people to unacceptable levels of risk. In 2017, a Queens landlord was accused of sending a tenants' personal information to ICE

---

[16] Lyla Renwick-Archibold, *Facial Recognition Locked Me Out of My Own Apartment. NYS Must Ban It*, AMSTERDAM NEWS, May 30, 2024, https://amsterdamnews.com/news/2024/05/30/op-ed-nys-must-ban-facial-recognition.
[17] *Id.*
[18] Sam Himmelstein, *What Are the Rules for Evicting Rent-Stabilized Tenants in NYC?*, BRICK UNDERGROUND, Dec. 8, 2021, https://www.brickunderground.com/rent/rules-for-evicting-rent-stabilized-tenant-nyc; Douglas MacMillan, *Eyes on the Poor: Cameras, Facial Recognition Watch Over Public Housing*, WASH. POST, May 16, 2023, https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing.
[19] Maggie Harrison Dupré, *Facial Recognition Used to Evict Single Mother for Taking Night Classes*, FUTURISM, May 17, 2023, https://futurism.com/facial-recognition-housing-projects.
[20] MacMillan, *supra* note 18.

after that tenant filed a discrimination complaint against him.[21] While New York City Human Rights Law prohibits discriminating or harassing tenants based on immigration status or origin, the current environment demonstrates the need for stronger, preemptive protections. While immigrant New Yorkers live in a city where landlords are allowed to collect their biometric data, they may be at risk of wrongful detention.

The Council must act urgently to pass these bills to live up to its commitments as a sanctuary city and to protect all New Yorkers, particularly New Yorkers of color, from harm.

Sincerely,

Nina Loshkajian

Nina Loshkajian
Technology & Racial Justice Collaborative Fellow

[21] Lauren Cook, *Queens Landlord Gave Tenant Information to ICE After Discrimination Complaint, Commission Says*, AMNY, July 19, 2017, https://www.amny.com/news/queens-landlord-gave-tenant-information-to-ice-after-discrimination-complaint-commission-says-1-13810387.

Fight for the Future is a national digital rights nonprofit organization with over 85,000 members in New York City and over 3 million members globally.

Fight for the Future strongly SUPPORTS passing Intros 213-2026 and 428-2026, bills banning biometric surveillance like facial recognition in places of public accommodation and in residential buildings.

FFTF leads the Ban Facial Recognition coalition of more than 40 racial justice and human rights organizations. FFTF also leads the Ban Facial Recognition in Venues campaign, endorsed by 200+ artists including Tom Morello, Boots Riley, and Wheatus, as well as the Ban Facial Recognition in Schools campaign, endorsed by leading human rights groups such as the ACLU, STOP (Surveillance Technology Oversight Project), and Encode Justice.

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.

Facial recognition enables massive invasion of privacy at a previously impossible scale. It also systematically misidentifies people of color, trans people, and basically anyone who is not a white man.

Stores and businesses are already using this technology to keep their enemies out – soon enough, we will see stores using it to bar entry to anyone in an ICE database or anyone on food stamps, perpetuating historic and present day institutionalized racism.

Once companies collect this data, we have virtually no way of knowing how they'll use it. They can sell it to data brokers or share it with abusive law enforcement agencies. Databases of biometric information – unchangeable bodily data – have also already been hacked, posing unprecedented risks to people's privacy and safety.

Industry groups will claim the data they're collecting "isn't useful to hackers or anyone else," but that's not the case – when companies create systems for identifying people using facial recognition, law enforcement, hackers, and others can abuse and/or trick those systems to gain access to people's private data.

The city of Portland, Oregon, was the first to take the groundbreaking step of passing legislation that prevents the use of this tech in places of public accommodation, and now New York City has the opportunity to do the same—setting a national and global example.

The New York City Public Advocate, Jumaane Williams, and the former chair of the City Council's Committee on Consumer and Worker Protection, Marjorie Velázquez, have strongly

condemned the use of facial recognition in public places. And after studying the use of this tech in schools, the New York Department of Education concluded the harms of facial recognition far outweigh any possible benefits. Facial recognition has been banned in New York schools, and we urge the council to ban it in places of public accommodation and residential buildings.

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.

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 0213-2026 Res. No. 0428-2026

☐ in favor ☒ in opposition

Date: MARCH 2, 2026

(PLEASE PRINT)

Name: ROBERT JAFFAN

Address: 1455 PENNSYLVANIA AVE., NW #400 WASHINGTON, DC 20004

I represent: INTERNATIONAL BIOMETRICS & IDENTITY ASSN.

Address: (SAME AS ABOVE)

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 2138428 Res. No. _____

☒ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: NINA LOSHKAJIAN

Address: [redacted] NY, NY, 10024

I represent: CENTER ON RACE INEQUALITY AND THE LAW

Address: 139 MacDougal St, NY, NY, 10012

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 0213/2026 Res. No. _____
0428-2026

☒ in favor ☐ in opposition

Date: 3/2/26

(PLEASE PRINT)

Name: Sergio DE LA PAVA

Address: 100 William Street NY, NY

I represent: New York County Defender Services

Address: 100 William

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. 0213 Res. No. _____

☒ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: ~~Staff~~ SHRUTHI VELIDI

Address: [redacted] Astoria NY 11106

I represent: DSA Tech Action

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 213-428 Res. No. _____

☐ in favor ☑ in opposition

Date: _____

(PLEASE PRINT)

Name: JAKE PARKER

Address: 7455 Coleserville, Road 1200 Silver Spring, MD

I represent: Security Industry Association

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 213+248 Res. No. _____

☑ in favor ☐ in opposition

Date: 3/2/26

(PLEASE PRINT)

Name: Laura Moraff

Address: 49 Thomas St. New York, NY 10013

I represent: The Legal Aid Society

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: _____

correct title

(PLEASE PRINT)

Name: Alex Foard

Address: Assistant Commissioner, Research & Collaboration at OTI

I represent: _____

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: Beverly Blondmonville

Address: [redacted]

I represent: _____

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: Michele Blondmonville

Address: [redacted]

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. 213/428 Res. No. _____

☑ in favor ☐ in opposition

Date: 3/6/26

(PLEASE PRINT)

Name: Medha Raman

Address: 125 Broad St 19th Fl New York, NY 10004

I represent: New York Civil Liberties Union

Address: 125 Broad St 19th Fl New York, NY 10004

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: Talia Kamran

Address: 177 Livingston St

I represent: Brooklyn defender services

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: 2 March 2026

(PLEASE PRINT)

Name: Cynthia Conti-Cook

Address: _____

I represent: Collaborative Research Center for Resilience

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. 428 Res. No. _____

☐ in favor ☐ in opposition

Date: 3/2

(PLEASE PRINT)

Name: Lucy Joffe

Address: _____

I represent: NYPD

Address: 100 Gold St

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. 213 / 428 Res. No. _____

☒ in favor ☐ in opposition

Date: 3/2/20

(PLEASE PRINT)

Name: Corinne Worthington

Address: 75 New York Ave, Brooklyn

I represent: Surveillance Technology Oversight Project

Address: _____

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