

**NEW YORK CITY CYBER COMMAND TESTIMONY BEFORE THE NEW YORK
CITY COUNCIL COMMITTEE ON TECHNOLOGY**

“CYBERSECURITY OF NEW YORK CITY AGENCIES”

JUNE 10, 2024

Good morning, Chair Gutiérrez and members of the City Council Committee on Technology. Thank you for inviting me today and allowing me an opportunity to speak on the work of NYC Cyber Command. My name is Kelly Moan. I am the Chief Information Security Officer for the City of New York and head of New York City Cyber Command, under the Office of Technology and Innovation (OTI). With me is Chantal Senatus, OTI’s Deputy Commissioner for Legal Matters.

Since its inception in July 2017, New York City Command has played a vital role in protecting and defending the city and its residents from the impacts of cyberattacks. Over the past seven years, we have built out security services and increased the cyber maturity at over 100 city agencies. We work collaboratively with agency partners, as well as state, federal, and private entities, to safeguard the essential services and data that New Yorkers depend upon daily. The City Council, as I am sure you are aware, recognized the significance of our duty when it voted unanimously to add Cyber Command to the New York City charter in 2020.

Our mission – the one that inspires me and my talented team – is to make New York City the most cyber resilient city in the world. This is no small endeavor. New York City is America’s financial, cultural, and media capital; and the size and the scale of the city ecosystem rivals that of most states or federal agencies. NYC is also a target for cyberattacks with a technology landscape that is unparalleled among other cities and states. This requires a unified, comprehensive defense against constant cyber threats, and partnerships across public and private sector– as well as the support of the administration and the members of this council.

At the outset of his administration, Mayor Adams signed Executive Order 3 in January 2022 to consolidate the city’s technology agencies, including New York City Cyber Command, into the newly created Office of Technology and Innovation

(OTI). One month later, Mayor Adams signed Executive Order 10, which further established the roles and responsibilities of Cyber Command, including:

- Setting information security policies and standards for the city
- Directing the city's citywide cyber defense and incident response
- Deploying defensive technical and administrative controls
- AND providing guidance to City Hall and city agencies on cyber defense.

Executive Order 10 also directed each agency appoint a Cyber Command Liaison to interface with us to strengthen collaboration and expand incident response capabilities. As a result, we launched NYC Cyber Academy, a specialized training program to bolster the city's cybersecurity workforce and enhance agency cyber capability. To date, we have graduated public servants from 50 city agencies in three cohorts, with a fourth cohort currently underway.

In February 2022 – the same month that he signed EO10 – Mayor Adams joined with Governor Hochul to launch the first-of-its-kind Joint Security Operations Center in Brooklyn. This 24/7/365 cybersecurity hub, situated inside of NYC Cyber Command's Security Operations Center, allows us to coordinate real-time efforts with city, state, and federal entities in ways that bolster the defenses of both New York City and the broader New York State.

As part of NYC Cyber Command's role, we provide a number of services to city agencies and assist in implementation of key work-streams to bolster agencies' cyber maturity. These range from technical controls such as security tools to administrative controls, such as policies and procedures. Cyber Command has also consistently worked with city agencies and elected offices to develop cybersecurity roadmaps that prioritize the critical cybersecurity work undertaken by these offices.

In October 2023, New York City launched our Vulnerability Disclosure Program (VDP), the first of its kind for our city and the largest for a U.S. municipality, broadening the scope of the city's efforts to identify and address vulnerabilities

within its publicly accessible digital resources. The VDP enables IT developers and security researchers to identify vulnerabilities in City-owned websites and systems and responsibly disclose them. It provides rules of engagement and guidelines for submission, and the program complements existing Cyber Command initiatives that facilitate timely remediation of identified risks.

I also want to underscore to the Council that our collaboration extends beyond government partners. Roughly 85% of U.S. critical infrastructure is private, so here in New York we have focused on partnerships with the private sector as well. This means collaborating with banks, hospitals, utilities, among many others, to maintain our collective cyber resilience through cyber threat intelligence sharing and joint tabletop exercises.

As the City's Chief Information Security Officer, I am honored to serve alongside my dedicated team, and our city agency teams, in furtherance of this critical mission. New York City Cyber Command's expanded organizational structure and alignment within OTI have placed the team in a strong position to monitor and respond to wide-ranging cyber threats.

But, as we are all keenly aware, there's no time for victory laps when it comes to cybersecurity. The work is never over, and there are no absolutes. There are no assurances that security and operational control measures will be successful in safeguarding against all cyber attacks. New cyber threats are discovered daily with increasing sophistication and complexity.

In cybersecurity, minutes matter; having strong partnerships in place prior to an incident, across many different sectors, are essential.

Cybersecurity is a team sport, and New York City Cyber Command is only one part of that team. Through continuous education to increase awareness of social engineering tactics, our cyber-aware city workforce is also a key line of defense to help prevent cyberattacks. They stand vigilant and trained to report suspicious activity expeditiously.

As we look to the future, we will continue to promulgate a holistic approach to strengthen NYC's defenses and adapt to a constantly evolving landscape.

I will now turn briefly to the pieces of legislation for today's hearing.

Intro 425 seeks to amend the administrative code of the city of New York, in relation to limiting the use of biometric recognition technology in certain residential buildings. To the extent that this legislation concerns the use of such technology on private property, it is not within OTI's purview.

Intro 217 seeks to amend the administrative code of the city of New York to prohibit places or providers of public accommodation from using biometric recognition technology and to protect any biometric identifier information collected. To the extent that this legislation has specified that it does not apply to the use of biometric identifier information by government agencies, employees, or agents, it is not within OTI's purview.

While OTI is unable to take a position on these bills, we want to underscore the Administration's commitment to work with City Council and ensure the proper balance of privacy and public safety with emerging technology.

Intro 539 seeks to prohibit telecommunications carriers and mobile application developers from sharing a user's location data with another person, if the location is within New York City. This bill would also impose monetary penalties for violation of the provision and proposes that the Department of Information Technology and Telecommunications enforce this measure. Although OTI supports the Council's efforts to address privacy concerns, implementation of this legislation, as drafted, would not be possible. OTI would welcome discussion relating to the intended framework for enforcement under these provisions. Additionally, OTI regulates the rights of way for telecommunications infrastructure and does not regulate mobile application developers.

I thank Chair Gutiérrez and committee members for your time and the opportunity to testify. I am happy to take any questions.

###

Testimony: The Use of Biometric Identification Systems

6.10.24

NYC COUNCIL COMMITTEES ON TECHNOLOGY & CIVIL AND HUMAN RIGHTS

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

Facial and biometric recognition technologies can provide strategic uses in many aspects of daily life and business. As technologies that focus on security or crowd safety features continue to develop, they have the potential to help businesses in new ways -- many of which are still unforeseen. NYC's existing law requires public notification when these technologies are used by certain businesses, and it is important for any businesses using them to do so with complete transparency and respect for personal privacy. While the use of biometric recognition technology is not widely seen in housing developments, we do believe it is important to maintain the option for property owners to have reasonable and responsible access to new technologies. While the roll-out of new facial and biometric recognition technologies could result in unforeseen circumstances, Tech:NYC also recommends any new legal or regulatory limitations to be developed with responsible use cases in mind.

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

There are already many innovative products and services that use facial and biometric recognition technologies, which are being used in homes and businesses across the country, and provide cost effective security solutions. Off-the-shelf home and business safety devices, like smart cameras, now

have technology that can recognize faces, which help to track who is entering or requesting to enter a premise. Facial and biometric recognition can aid businesses implementing new customer service and security measures, as well as those which have been targeted for crimes or need to flag individuals with restraining orders or other legal prohibitions.

Facial and biometric recognition technologies are often used by businesses and venues that have large numbers of customers or visitors, and can be used to count the number of visitors or patrons of large events or certain businesses. Their usage is often seen in the travel, sports and entertainment sectors, where the technology can provide more seamless access to venues and services. Banking is also a sector that is quickly implementing biometric recognition tools, which will help to reduce fraud while modernizing ATM and mobile banking technology. While there are ongoing concerns regarding bias and fairness of facial and biometric recognition technologies, it's important for the private and public sectors to work together to ensure that balanced frameworks are developed that allow the technology to be used responsibly. Regardless of the type of business or venue using these technologies, it is also crucial that there is full disclosure to the public on when they are used, and that patrons, customers and the public have a choice on when they can use them for accessing venues, businesses, or services.

Regarding Int. 217, various businesses and venues use facial and biometric recognition technologies at points of entry and prior to sales being made, especially when used to supplement or act as security measures. These practices conflict with the goals of this bill, and would create substantial compliance efforts and costs to incorporate written consent of consumers into security practices. It would also prove detrimental to conducting business and providing customer support should this technology be prohibited from the practices of identifying or verifying customers. The separate security and disclosure provisions for biometric data in this bill are a helpful step to ensure the information collected is secure. Int. 425 similarly places premature burdens on residential developments, which should have the opportunity to explore technological solutions relating to security and modernization, especially for buildings that do not have the budget to support full time security or entrance staff. Property technology companies, also known as "proptech" are a rapidly growing sector in New York, and rely on our local real estate and construction industries for partnerships to continue developing new services and technologies.

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



Shahana Hanif

CITY COUNCIL MEMBER, DISTRICT 39

Opening Statement of Council Member Shahana Hanif- Committee on Technology

June 10, 2024, City Hall- Council Chambers, 10AM

Thank you to Chair Gutiérrez for holding today's important hearing and for including my bill, [Intro. 217](#), on today's agenda. I am proud that 18 members of the Council currently sponsor this bill, including co-prime sponsors Chair Gutiérrez and Council Members Rivera, Williams, Sanchez, Louis, and Marte.

Intro. 217 would prohibit businesses and other places of public accommodation from using facial recognition and other forms of biometric surveillance to verify or identify a customer.

This measure is critical to combatting wrongful discrimination. Facial recognition tools have consistently been shown to have significantly higher inaccuracy rates for people of color and women. This has resulted in people in these populations being falsely accused of wrongdoing and denied access to public spaces.

It is also a matter of basic privacy. People have a right to access essential places like grocery stores without having their personal biometric information—like the shape of their face and the way that they walk—collected, used, or sold for targeted advertising or other purposes.

Since this bill was heard last session, there have been countless developments that have made the passage of this bill more urgent than ever including wrongful arrests and data leaks. But the event that stands out the most to me is the Federal Trade Commission's finding in December that the pharmacy chain Rite Aid used facial recognition technology to falsely and disproportionately identify thousands of people of color and women as likely shoplifters in its stores, including those in New York City.

The FTC describes the pattern as follows: "Acting on false positive facial recognition matches, employees followed customers around its stores, searched them, ordered them to leave, called the police to confront or remove consumers, and publicly accused them, sometimes in front of friends or family, of shoplifting or other wrongdoing." In one case, a false match resulted in a 11 year old girl being wrongly stopped and searched.

I urge those here today to imagine how dehumanizing it would be to one of these customers. The FTC finding emphasizes the discrimination and harm caused by biometric surveillance is not a paranoid hypothetical or a one-off incident. It is here, it is real, and we need to act. While Rite Aid is now prohibited from using biometric surveillance for the next five years, we shouldn't need a federal investigation and lawsuit to prohibit other businesses from replicating this practice and victimizing more New Yorkers.

I want to stress that the bill takes a measured approach. If passed, customers would be still able to opt-in to uses of technology such as pay-by-palm at a grocery store checkout or a



Shahana Hanif

CITY COUNCIL MEMBER, DISTRICT 39

biometric travel document verification at the airport. Additionally, businesses that truly need to collect and use biometric technology to carry out core functions, such as a custom running shoe store that uses gait analysis, would be permitted to do so. We are pushing for basic consumer protections, not ideological absolutism.

Additionally, I want to make it clear that this bill does not impact normal security tools like video monitoring. I share concerns around retail theft and repeat offenders and encourage the City to support our small businesses with funding for infrastructural security upgrades. However, as evidenced by the Rite Aid case, biometric surveillance is not an effective tool and in many ways can make New Yorkers less safe.

I reject the premise that facial recognition is an essential security measure. As a Muslim New Yorker who grew up in the post-9/11 era, I am all too familiar with the negative consequences of using fear to justify excessive and biased surveillance.

I want to thank the incredible Ban The Scan coalition with whom we rallied outside earlier today and who are here to testify in support of Intro. 217. This broad and diverse coalition of racial justice leaders, civil and human rights institutions, and technology experts underscores the necessity of this bill.

I also want to state my support for Council Member Rivera's Intro. 425—which I am proud to co-prime sponsor—and amplify the coalition's call for future legislation that would ban city government use of biometric surveillance as well.

I'll now pass it back to Chair Gutiérrez.



JUMAANE D. WILLIAMS

**STATEMENT OF PUBLIC ADVOCATE JUMAANE D. WILLIAMS
TO THE NEW YORK CITY COUNCIL COMMITTEE ON TECHNOLOGY
JUNE 10, 2024**

Good morning,

My name is Jumaane D. Williams, and I am the Public Advocate for the City of New York. I would like to thank Chair Gutiérrez and the committee members for holding this hearing.

New technologies can come with the potential erosion of privacy rights and we cannot stand by with the proliferation of these technologies. While many have accepted decreasing privacy rights as an inherent tradeoff with receiving faster services, technology should never threaten our safety.

I support bills Int 0539, Int 0425, and Int 217, because we must hold individuals and businesses accountable for potentially putting lives at risk through the implementation of biometric and location sharing technologies. There must be strong regulations in place for utilizing biometric technologies, in no small part because this technology has been proven inaccurate in accurately identifying women and people of more color.

Researchers at MIT reported in January 2019¹ that facial recognition software marketed by Amazon misidentified darker-skinned women 31% of the time, while other studies have shown “*algorithms used in facial recognition return false at a higher rate for African Americans than white people unless explicitly recalibrated for a black population.*”² Specifically, the Amazon technology misidentifies people with darker complexions 15% of the time as compared to only 3% for people with lighter complexions³. These findings prompted experts at Google, Facebook, and Microsoft to sign a letter calling on Amazon to stop selling its facial-recognition technology to law enforcement⁴. Int 217 and Int 425 correctly recognize the danger of biometric data collection, and place restrictions on the usage.

Specifically, landlords utilizing biometric technology will lead to unnecessary police confrontations since landlords permitted to use this technology could easily determine who can enter the building through an inaccurate test. Additionally, there are landlords who harass tenants to deregulate an apartment, and may use the technology to further those goals.

With mass surveillance, personal information is more likely to be at risk if a cyber security attack occurs since it is continuously collected and stored. This is especially relevant to

¹<https://www.technologyreview.com/2019/01/29/137676/making-face-recognition-less-biased-doesnt-make-it-less-scarey/>

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

³ Ibid 1

⁴<https://medium.com/@bu64dcjrjtwitb8/on-recent-research-auditing-commercial-facial-analysis-technology-19148bda1832>



JUMAANE D. WILLIAMS

Intro 539, because data being sold to third parties can lead to the development and expansion of poorly monitored databases. For a recent example from April 2024, Home Depot utilized a third-party software platform to process employee information, and the third party company's data leak released Home Depot employees staff's names and work email addresses⁵. While there has been no reported incidents as a result of the leaks, there are serious consequences. Data leaks of names and email addresses are used for online criminals to try phishing attempts and cyberattacks. In this instance, both the safety of employees and of the company are in jeopardy.

It is no exaggeration to say that leaks of personal data can put peoples' lives at risk. Commuting patterns, frequent locations, or other identifying information threatens survivors of domestic violence as well as anyone in a marginalized group who may be targeted. For example, in the United Kingdom a domestic violence survivor had to be immediately moved after their location was exposed in a data leak⁶.

Facial recognition technology, unrestricted access to location data, and biometric technology's harms far outweigh many positives. As lawmakers we have a responsibility to curb abuses of surveillance technology, and these bills are a good step in the right direction.

Thank you.

⁵ <https://www.retaildive.com/news/home-depot-confirms-data-breach-employee/712678/>

⁶ <https://theconversation.com/for-domestic-violence-victim-survivors-a-data-or-privacy-breach-can-be-extraordinarily-dangerous-216630>

REBNY Testimony | June 9, 2024

The Real Estate Board of New York to The City Council Committee on Technology on Biometrics Legislation

The Real Estate Board of New York (REBNY) is the City's leading real estate trade association. Founded in 1896, REBNY represents commercial, residential, and institutional property owners, builders, managers, investors, brokers, salespeople and other organizations and individuals active in New York City real estate. We appreciate the opportunity to testify on several bills pertaining to the collection and use of biometric data and technology.

Bill: Intro 217-2024

Subject: This legislation addresses the use of biometric identifier information and biometric recognition technology by place or providers of public accommodation such as retail stores. The bill would ban the use of biometric recognition technology in such place, require written consent from customers prior to data collection, and regulate the use and storage of biometric identifier information while requiring the development and implementation of reasonable safeguards to protect collected data. These safeguards include conducting risk assessments for the various systems that handle such information, testing and monitoring safety systems, and protecting against unauthorized access to biometric data. Lastly, this legislation ensures that violations of these provisions will be subject to penalties and allow individuals to bring private rights of action.

Sponsors: Shahana K. Hanif, Jennifer Gutiérrez, Carlina Rivera, Nantasha M. Williams, Pierina Ana Sanchez, Farah N. Louis, Christopher Marte, Chi A. Ossé, Shekar Krishnan, Julie Won, Alexa Avilés, Yusef Salaam, Erik D. Bottcher, Amanda Fariás, Sandy Nurse, Crystal Hudson, Carmen N. De La Rosa

REBNY appreciates the intent of this legislation, given concerns that the collection and use of personal biometric data has the potential to infringe on personal privacy rights. However, an outright ban on the use of biometric recognition technology to identify or verify customers seems to go too far, as there are circumstances where such technology can be used for efficient and effective security measures – for instance to combat retail theft which continues to be of concern to many small businesses across the city. In addition, the

consent requirements are likely unattainable for many establishments with large customer bases. The proposed disclosure and opt-out provisions should be sufficient on their own and as such the consent requirements are unnecessary.

Bill: Intro 425-2024

Subject: This bill would disallow owners of multiple dwellings from installing, activating, or using biometric recognition technology that identifies tenants and/or guests.

Sponsors: Carlina Rivera, Pierina Ana Sanchez, Tiffany Cabán, Shahana K. Hanif, Farah N. Louis, Shekar Krishnan, Julie Won, Alexa Avilés, Yusef Salaam, Gale A. Brewer, Erik D. Bottcher, Amanda Farías, Christopher Marte, Chi A. Ossé, Carmen N. De La Rosa, Selvena N. Brooks-Powers, Crystal Hudson, Sandy Nurse, Nantasha M. Williams, (by request of the Manhattan Borough President)

REBNY appreciates the intent of this legislation. However, the wholesale ban of certain information collection systems, including those that can identify tenants, is excessive. Many residents appreciate the ease with which they are able to enter buildings but also recognize the protections afforded to them by the use of such technologies. Among other benefits, these systems can be used to provide effective and efficient security measures for tenants and guests. Instead of a ban, the Council should consider thoughtful regulation of how such data is collected, used, and shared with others.

CONTACT:

Maya Kurien

Vice President of Advocacy
Real Estate Board of New York
mkurien@rebny.com

Daniel Avery

Director of Policy
Real Estate Board of New York
davery@rebny.com



June 10, 2024

CHIP Testimony on Int 425-2024 Biometrics Bill

Thank you for holding this hearing today. I am Adam Roberts, Policy Director for the Community Housing Improvement Program (CHIP). We represent New York's housing providers, including apartment building owners and managers. Our members operate rent-stabilized housing, which contains 1 million units of housing in New York City, making up 40% of its rental housing and the vast majority of its affordable housing.

Int. 425 is punitive to tenants who live in rent-stabilized housing, as well as workers, including our members, who operate rent-stabilized housing. Rent-stabilized buildings generally do not have the financial resources to hire full-time doormen. Even so, affordable housing must also be safe housing.

This is particularly notable as rent-stabilized housing is in the midst of a major financial crisis. Across the city, net operating income is in a freefall, dropping as much as 20% in the Bronx year over year. The largest lender to rent-stabilized housing, Signature Bank, collapsed last year. Meanwhile, the now-largest lender, New York Community Bank, has been saved by collapse by Trump's former Treasury Secretary, Steve Mnuchin, who has threatened to foreclose on our members en masse.

The affordability rent-stabilized housing provides is entirely unsubsidized by the government. This means rent-stabilized housing does not have the operating revenue to cover basic expenses, let alone hire full-time doormen. Even if the financial crisis were to end, many buildings are too small to ever financially support full-time doormen.

Therefore, rent-stabilized tenants and workers rely on more affordable security systems, such as virtual doorman and CCTV systems, to ensure their buildings are secure. In the future, they likely will use biometric identifiers like fingers, voice, irises, and facial recognition. They too are more affordable than full-time doormen.

This bill is so broadly written, that it bans any technology which "can be used to... establish individual identity." Every security system from virtual doorman systems to fingerprint scanners will be illegal. Technologies which "established individual identity" have been used for decades to ensure safety in buildings which lack full-time doormen. We cannot imagine how tenants and workers will react to seeing CCTV and virtual doorman systems removed because of this bill.

The City Council will be depriving rent-stabilized tenants and workers the safety which wealthy New Yorkers enjoy in their homes.

Again, thank you for holding this hearing today.



MEMORANDUM

DATE: June 7, 2024

TO: Chair Jennifer Gutiérrez and Members of the Committee on Technology;
New York City Council

FROM: Jake Lestock, Director of State Legislative Affairs

RE: Opposition to Int. No. 539

CTIA®, the trade association for the wireless communications industry, opposes Int. No. 539.

- **This legislation will only increase customer frustration without any discernable benefit**
- **There is robust Federal oversight and it is working**
- **Mobile service providers have adapted their business practices, but they are not exclusive data gatekeepers**

To best protect consumers, privacy protections should apply consistently and should not be technology- or sector-specific

- The bill is confusingly limited to the sharing of location data by only a subset of entities within the online ecosystem – location data shared by telecommunications carriers and mobile app developers – regardless of who collected the data. Consumers are unlikely to understand or expect this limited protection, which does not reflect the reality of modern data processing, in which online data flows seamlessly across the internet ecosystem among various companies and technologies.
- The bill would not apply to the sharing of location data shared by other entities throughout the internet ecosystem, such as web browsing outside of mobile devices, connected vehicle technology, wearables, or other connected devices. Consumers are unlikely to understand, appreciate, or expect this outcome.
- Because the proposed law would not apply in all situations, other entities could collect, sell, and disclose large amounts of location data in other ways. This will promote anti-competitive outcomes in the marketplace. Communications providers are not the gatekeepers to location data in the online ecosystem.
- The bill would apply to individuals within New York City, meaning persons present in the city rather than residents of New York City. Having the law apply to persons present in New York City rather than residents of the city would also create consumer confusion and creates a significant operational challenge.

The Legislation Will Require Companies to Collect More Data, Not Less

- Because of the way this bill is drafted to require communications providers to limit the sharing of location data of individuals within New York City, it mandates anti-privacy outcomes because more data will have to be collected and linked to individuals to determine when they are located within the city and when the obligations apply. It also creates an onerous requirement for carriers to set a geofence around the city and apply the bill's rules to consumers while they are present in the city, and then maintain data on compliance in the event of potential litigation.
- To the extent the bill operationally requires carriers to apply its standards in other states, it likely violates the Dormant Commerce Clause of the United States Constitution.

This legislation could increase consumer frustration and make it difficult for businesses operating in New York City to provide important services to consumers

- This legislation would add to consumer frustration and notice fatigue in which consumers stop paying attention – but businesses would still be faced with the burden of presenting and recording the consents called for by the bill.
- The bill applies to any location data – not just precise or technologically derived data. This would add to the number of consents required from consumers, adding to consent fatigue and likely causing customer confusion when asked for consent to share for routine purposes.
- The bill would also apply to any location data irrespective of who collected the data. In combination with the breadth of the definition of location data, this would put businesses in the nearly impossible position of determining whether a consumer's address provided to it by a third party was originally collected while the consumer's device was present in New York City while not placing any burden on that third party with respect to the collection of that data.
- The bill broadly limits any disclosure and not just the sale of location data. Yet many businesses use location information to identify and combat fraud for the benefit of customers. This bill could impede these legitimate, important, and critical business operations.
- As a direct result, bad actors will have a much easier time fraudulently using the identities of New York City residents and committing other frauds and bad acts and the potential for disruption in services to consumers will be greatly heightened. Simply put, bad actors will not consent to having their data used for these detection purposes.

Federal & state laws already exist providing consumer protections

- The Federal Trade Commission's (FTC) Privacy Framework considers precise geolocation information to be sensitive, meaning that its collection must be subject to opt-in consent. The FTC has brought enforcement actions against companies that have misrepresented consumer control regarding the collection of geolocation data. Examples include actions against [Nomi Technologies](#) and [Goldenshores Technologies](#) (involving the flashlight app).
- The Federal Communications Commission (FCC) regulates wireless carriers' use of Customer Proprietary Network Information (CPNI), which includes certain location information.
- The New York Attorney General (AG) also has the authority to address unfair or deceptive acts or practices relating to consumer privacy under New York's consumer protection laws.

A private right of action would harm businesses with no benefit for consumers

- This bill allows for a private right of action, which will unfairly expose wireless providers in New York City to costly litigation that will benefit the plaintiff's bar while offering little relief to consumers.
- Instead of allowing for a private right of action, New York City's Department of Information Technology and Communications should shape statewide policy with a holistic and experienced approach, which will best encourage compliance, support innovation, and prevent and remediate harm; consistent interpretation and application of the law will benefit both businesses and consumers.

Activity on consumer privacy is taking place in the New York State Legislature and Congress

- A uniform law that covers all types of personal data and the different companies that collect it is the best approach for U.S. consumers and momentum for this type of baseline legislation that would offer consistent protections for all U.S. consumers has been building. Indeed, the New York legislature is expected to consider comprehensive privacy legislation next session.
- There is bipartisan interest in consumer privacy in the current Congress; hearings have been held and many of the concepts in bills pending in the Senate and the House have widespread support.



- The FTC has released their advance notice of proposed rulemaking (ANPR), titled Trade Regulation Rule on Commercial Surveillance and Data Security – an effort to build a robust public record to inform whether the FTC should issue rules to address privacy practices if sufficient momentum should not occur in Congress.



Testimony in Support of Int 0217 and Int 0425

Committee on Technology
June 10, 2024

Good morning, my name is Hally Thornton. I've been a resident of New York City for 14 years and am testifying today on behalf of [Fight for the Future](#) in support of banning facial recognition in public places and residential buildings.

Fight for the Future is a digital rights organization with over 2.5 million members nationwide, including over 85,000 in New York City. I'm a staff member focused on administrative and campaign support.

Our group is strongly opposed to the use of technologies that collect people's biometric data and store that data en masse in the cloud. This includes the facial recognition tools used in places of public accommodation and residential buildings.

[Studies](#) have [repeatedly](#) shown that facial recognition programs simply don't work well and systematically misidentify basically anyone who isn't a white man, putting people of color, women, and even kids at risk of harassment and wrongful arrests—events that can forever change the course of someone's life.

But let's be clear, facial recognition is just as dangerous when it actually works. 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](#). Facial recognition technology enables mass monitoring and tracking at a previously impossible scale, so each time biometric data is shared or leaked, it brings us one step closer to an authoritarian world in which everyone is identified wherever they go.

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 – if companies create systems for identifying people (who are otherwise anonymous) using facial recognition, then law enforcement, hackers, and others can abuse and/or recreate those systems.

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.

As the New York Department of Education [concluded](#) after studying the use of this tech in schools, 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.

Advocates of the
Food Industry
Since 1900



FOOD INDUSTRY ALLIANCE OF NEW YORK STATE, INC.

111 Washington Avenue - Suite 200, Albany, NY 12210 (518) 434-1900

**Testimony from the Food Industry Alliance of New York
NYC Council Oversight Hearing: Cybersecurity of New York City Agencies**

June 10, 2024

The Food Industry Alliance of New York State (FIA) is a nonprofit trade association that advocates on behalf of grocery, drug and convenience stores throughout the state. Within our membership includes the broad spectrum of the New York City retail food sector, from independent neighborhood grocers to large chains, including many unionized stores.

We appreciate the opportunity to submit this formal testimony expressing our opposition to Int. 0217-2024, which prohibits the use of biometric recognition technology by a place of public accommodation to verify or identify a customer. It also creates numerous new conditions on the collection of biometric identifier information that are so far reaching that they effectively bar the accumulation of such information by the city's grocers.

For example, under proposed section 22-1202(a), any place of public accommodation that collects or otherwise obtains biometric identifier information of customers must get the written consent of each customer before any collection. This is, of course, impossible in a grocery store context and the exemption provided in proposed section 22-1204(c) does not apply to grocery stores. In addition, the bill contains no exceptions allowing biometric recognition technology to use biometric identifier information to verify or identify a customer for public safety purposes.

The inability to collect biometric identifier information and use biometric recognition technology would seriously undermine the ability of the city's grocers to deter shoplifting and assist law enforcement investigations of repeat offenders. The failure to reverse rising thefts at marginal grocery stores will likely result in the closure of those locations, thus exacerbating the city's food desert problem.

According to "FRESH By the Numbers," a February 2023 report prepared by the NYC Department of City Planning in partnership with the NYC Economic Development Corporation, in December 2021 the number of FRESH eligible zones was increased to parts of 11 additional Community Districts (on top of the zones in 20 Community Districts created at program inception in 2009), reflecting the stubborn prevalence of underserved areas in the city. The closure of marginal supermarkets due to rising theft would undermine the city's ongoing efforts to reduce the existence of food deserts through FRESH and other programs.

“Historical New York City Crime Data” obtained from the NYPD page on <https://www.nyc.gov/site/nypd/stats/crime-statistics/historical.page> reflects the recent surge in petit larceny complaints:

Year	Number of Petit Larceny Complaints
2000	93,785
2019	89,314
2020	82,101
2021	87,105
2022	115,658

The data shows an approximate 4.7% reduction in petit larceny complaints between 2000 and 2019, with an additional decline during the initial year of COVID, when quarantines and lockdowns were at their peak. That was followed by two years of increases in 2021 (about 6% compared to 2020) and 2022 (approximately 40% compared to 2020), for a two-year rise of about 46%. The 115,658 petit larceny complaints reported by the NYPD in 2022 are the largest between 2000 and 2022.

A rise in retail theft is accompanied by an increase in threats of violence and actual violence during the commission of such crimes. This creates the need for merchants to use legal, ethical methods that are not confrontational to deter theft and assist law enforcement investigations of repeat offenders. Biometric systems are focused on identifying recidivists who commit a disproportionate share of thefts.

According to an April 15, 2023, New York Times article titled *A Tiny Number of Shoplifters Commit Thousands of New York City Thefts*, “Nearly a third of all shoplifting arrests in New York City last year involved just 327 people, the police said. Collectively, they were arrested and rearrested more than 6,000 times, Police Commissioner Keechant Sewell said.” The goal of using a biometric system is to assist law enforcement in the investigation of repeat offenders, by identifying such individuals and/or providing evidence that can be used in an investigation.

Further, it is our understanding that the commercial use of facial recognition is legal in all 50 states. In addition, there is a current trend away from blanket bans of facial recognition technology. For example, Virginia, Cobb County (Georgia), New Orleans and Baltimore all reversed facial recognition restrictions in 2022. The trend toward expanded facial recognition includes appropriate privacy protections and exemptions for safety and security applications.

This is why we oppose this legislation and strongly support a collaborative effort to replace this bill with a new measure that will allow the collection of biometric identifier information, and its use through biometric recognition technology, that enables the identification of individuals for

the wellbeing and safety of customers and workers. In lieu of obtaining all but impossible individual customer permissions for their personal data, perhaps increased limitations on what can be done with this data after it is collected would serve as a viable alternative.

We look forward to participating in such a cooperative process with Councilmember Hanif and other government stakeholders.

Respectfully submitted,

A handwritten signature in cursive script that reads "mauracallahan".

Maura Callahan
Government Affairs Coordinator
Food Industry Alliance of NYS, Inc.



***Testimony of Robert A. Tappan
Managing Director
International Biometrics + Identity Association (IBIA)
Before the New York City Council
Monday, June 10, 2024***

Dear Committee Chair Gutiérrez and New York City Council Members:

Thank you for the opportunity to appear before you today to discuss bills number Int. No. 217-2024 and Int. No. 425-2024, regarding the regulation and use of biometric technologies in places of public accommodation as well as in residential buildings in New York City.

IBIA is an industry association whose Member companies design and manufacture biometric products and technologies that span a wide array of use-cases and different measurement types, known as modalities, which include: fingerprints, iris and retina, speech recognition, DNA, and facial recognition, among others. IBIA is chartered to advance the adoption and responsible use of these technologies for managing human identity to enhance security, privacy, access management, productivity, and convenience for individuals, organizations, and governments. We do this through advocacy, engagement, and education.

And that is why I am pleased to be back here before you today. This is my second time addressing the Council and this Committee on these important issues. I appeared before the Committee on Technology and the Committee on Civil & Human Rights on May 3 of last year to voice our concerns about the previous iterations of these two pieces of legislation.

IBIA and its members continue to have serious concerns with the language and scope contained in both bill numbers Int. No. 217-2024 and Int. No. 425-2024.

While we understand and respect the concerns around privacy and protecting civil liberties that have motivated these bills, an outright ban or severe curtailment on the responsible use of facial recognition would be an overreaction with severe unintended consequences. Facial recognition technology has become an integral tool for ensuring public safety, preventing and deterring crime, protecting citizens and visitors, and enhancing security and convenience across many sectors. Prudent regulation is required — not prohibition.

Facial recognition has proven invaluable for identifying suspects in violent crimes, human trafficking cases, shoplifting, finding missing persons and more. Proper policy guardrails,



combined with human oversight, can ensure that it is only used for legitimate purposes while protecting citizens' civil rights. A blanket ban on biometric technologies, as enumerated in these two bills, would be a step backwards. They would hamper commerce, as well as criminal investigations — and make New York less safe by depriving businesses and law enforcement of a powerful forensic tool.

In the private sector, facial recognition enhances physical security for offices, residential buildings, and facilities, not to mention acts as a secure method for accurate employee timekeeping. Retailers rely on it as part of their efforts to combat the rampant shoplifting plaguing this city and around the country. This property crime threatens the viability of local stores and food access in underserved areas when they are forced to close due to excessive losses. We should be enabling businesses and communities to address this public safety challenge, not tying their hands.

Rather than restricting all of the above beneficial biometric use cases, we should pursue a balanced regulatory framework to allow continuing innovation while ensuring strong civil rights protections. We would propose clearly defined rules authorizing facial recognition for strictly enumerated lawful purposes with proper transparency, human oversight, accuracy testing across demographics, data privacy safeguards, community involvement in policymaking, and mechanisms for redress. This measured approach could make New York a model for responsible use of facial recognition.

Regarding bill Int. No. 217-2024, the language contained outlining a specific Private Right of Action is more problematic, as we have seen in other jurisdictions like the State of Illinois' Biometric Information Privacy Act, or BIPA for short. With the seemingly earnest goal of regulating the collection and use of biometric data — just like these two pieces of legislation that we are addressing today — BIPA has instead been perverted and become a gambit for trial attorneys trying to milk legitimate companies who may have unwittingly violated the ordinance. Laws such as BIPA have been shown to serve no public good except merely to enrich plaintiffs and their lawyers, as well as to bankrupt companies just trying to do legitimate business.

What is needed is national legislation at the federal level is required to preempt state laws (including those in Illinois, California, and others) and establish a 50-state, uniform, safe and reasonable framework for uses of biometrics, including facial recognition. On behalf of IBIA and its Members, I urge you to support regulatory efforts at the federal level, and carefully reconsider what should be done locally. A patchwork of 50 different state laws and regulations, not to mention the myriad number of regulations being contemplated at the city and local level, all of whom differ from jurisdiction to jurisdiction, creates nothing but confusion and a complex set of booby-traps that hinders commerce, stifles economic development and innovation, and creates general confusion.



We believe that biometric technologies should never be subject to bans, or there will be unintended consequences for commerce, convenience, and the security of our citizens. We urge the Council to reject calls for a sweeping prohibition of facial recognition and instead enact robust guardrails enabling society to reap the powerful public safety and economic benefits of this technology while ensuring strong civil rights protections. IBIA would be pleased to work with you and your colleagues on the Council to develop sound policies that address these two concepts.

Thank you, respectfully, for your time today, Chairwoman Gutiérrez and all of the Council members gathered here today. I can take any questions if you wish.

I would also respectfully request that my testimony (plus any relevant attachments or citations whose length would have exceeded the time limit on oral testimony) be included for the record.

Thank you again.

#



June 10, 2024

**Testimony of Nelson Eusebio
Director of Government Relations
National Supermarket Association**

Before the

New York City Council Committees on Technology and Civil and Human Rights

Regarding

Int. 0217-2024

Thank you, Chair Gutierrez and the rest of the committee members, for the opportunity to submit testimony. My name is Nelson Eusebio and I'm the Director of Government Relations for the National Supermarket Association (NSA). NSA is a trade association that represents the interest of independent supermarket owners in New York and other urban cities throughout the East coast, Mid-Atlantic region, and Florida. In the five boroughs alone, we represent over 400 stores that employ over 15,000 New Yorkers. Our members work hard every day to run their businesses, support their families and provide jobs, healthy food, and full service supermarkets to their communities. Most of our members are of Hispanic descent and operate locations in underserved neighborhoods that have been abandoned by large chain stores.

My testimony today will focus on Int. 217 in "relation to prohibiting places or providers of public accommodation from using biometric recognition technology and protecting any biometric identifier information collected." Int. 217, sponsored by Council Member Hanif, would make it unlawful for any place or provider of public accommodation to use biometric recognition technology to verify or identify a customer. It would also require places or providers of public accommodation to notify customers if biometric identifier information is collected and to require written consent before any biometric recognition technology could be used. Additionally, the bill would require any such information collected to be protected and for written policies regarding its use to be made available.

The NSA supports holding bad actors who attempt to use biometric recognition technology to violate the privacy and rights of customers accountable. However, we are extremely concerned that prohibiting the use of this technology as a means to verify or identify a customer will make our supermarkets, as well as other businesses across the City, less safe and more vulnerable to would-be wrongdoers. At a time where our small, local businesses are facing upticks in shoplifting and assaults throughout the five boroughs,

the City should be looking to expand the resources available to keep our communities secure, not limit or outlaw them. We currently have stores that use facial recognition technology responsibly. They have caught repeat shoplifters before they were able to enter the store, protecting both employees and customers alike.

In addition, requiring written consent before utilizing any biometric recognition technology is an unreasonable hardship on employees who are already forced to be the first line of defense against those who attempt to do harm to our businesses and an inconvenience to shoppers who are simply trying to go about their day and purchase their necessities.

Consumers have already been driven to do their shopping online as a result of merchandise being locked behind glass or counters and having to wait extended periods for an employee to get them what they need. We want to be clear: we believe in holding those who would abuse this technology in an attempt to violate the rights of others accountable, and we believe in the Council's authority to protect the privacy of consumers. However, we respectfully believe that this well-intentioned legislation misses the mark when it comes to safeguarding both businesses and consumers in regard to crime and ensuring that the mom and pop shops, including the neighborhoods which they sustain, are a safe haven for all. The NSA welcomes the opportunity to discuss this legislation further and will make ourselves available to do so, for everyone to be protected.

Thank you.



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

Testimony of Daniel Schwarz
On Behalf of the New York Civil Liberties Union
Before the New York City Council Committee on Technology in Support of Intros.
217 and 425

June 10, 2024

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

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

The Council must ensure New Yorkers are not surveilled, targeted, discriminated against, and criminalized on the basis of invasive, flawed, and biased technology. To this end, we call for prohibitions on biometric surveillance in areas of severe power imbalance, including its use by law enforcement or other government agencies, in housing, and in other areas where our fundamental rights are at stake or where informed consent cannot be given. The NYCLU supports the two bills before the Committees, Introduction 217-2024, which would ban biometric surveillance in places of public accommodation and set clear rules for the collection of biometric data, and Introduction 425-2024, 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 deployment of facial recognition at Madison Square Garden to ban people from the stadium that had already purchased tickets³ illustrates the dangers from the growing surveillance industry and the urgent need for comprehensive privacy protections. And the planned installation of a facial recognition entrance system at the Atlantic Plaza Towers in Brownsville raised severe concerns about imposing invasive surveillance on residents and their guests.⁴ Fortunately, the tenants were successful in their advocacy against the landlord's plan and were able to stop the system from being deployed. Such a system raises significant concerns about misidentifications resulting in potentially dangerous interactions, privacy violations by precisely tracking the coming and going of every resident and their guests, building access issues, and heightened security risks due to the collection of biometric and movement data.

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

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

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

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

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

a security breach. And what we have witnessed so far should inspire little confidence in many companies' ability to adequately guard against misuse.⁵ Disclosing data policies, setting clear retention and deletion schedules, protecting against any third-party access, and establishing appropriate security mechanisms should be the baseline for anyone handling biometric data.

Biometric Surveillance by Law Enforcement

While the two 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 System⁶ and plans to increase that number to a staggering 50,000 cameras.⁷ And the NYPD continues to introduce even more cameras in the form of officer body-worn cameras and unmanned drones. It also makes use of social media photographs; in August of 2020, the NYPD used facial recognition software to identify a Black Lives Matter activist during a protest against police brutality through a photo from his Instagram account.⁸

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

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

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

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

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

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

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

photographs of celebrity lookalikes in lieu of actual suspect photos, editing suspect photographs (including through effects that substantially alter the suspect’s actual appearance) in order to generate a potential match, and apprehending suspects “almost entirely on the basis of face recognition ‘possible matches’” without taking additional investigative steps to establish probable cause.¹⁰

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

In another particularly alarming example, the Metropolitan Transportation Authority and the NYPD partnered with IBM to develop software to search for people by their skin color in the transit system.¹⁵ And Amazon Ring has partnered with hundreds of law enforcement agencies, including the NYPD, to facilitate data sharing from privately installed devices to the

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

¹¹ Joseph Goldstein & Ali Watkins, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database*, THE NEW YORK TIMES, Aug. 1, 2019,

<https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html>.

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

¹³ *Id.*

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

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

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

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

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

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

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

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

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

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

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

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

Introduction 217-2024 - Prohibiting places or providers of public accommodation from using biometric recognition technology and protecting any biometric identifier information collected.

Intro. 217 would amend the biometric disclosure for businesses law (Local Law 3 of 2021), Section 22-1201 of the Administrative Code, to prohibit places or providers of public accommodations from using biometric recognition technology to identify customers, and it would require written consent for any collection of biometric identifier information. It would further create transparency, security, and deletion requirements and ensure that customers are not treated or charged differently because they do not consent to the collection of their biometric data.

These changes add crucial protections to New York City law. As mentioned above, the deployment by MSG Entertainment across its sports and entertainment venues to target staff from law firms in litigation with MSG points to Orwellian use cases where it will be impossible to move and associate freely. And the technology's racial as well as gender bias risks disproportionately impacting women and people of color, such as in the misidentification of a Black teenager that barred her from entering an ice-skating rink²³ 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.²⁴ 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.²⁵ 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.

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

²⁴ James Clayton, *"I Was Misidentified as Shoplifter by Facial Recognition Tech,"* BBC, May 25, 2024, <https://www.bbc.com/news/technology-69055945>.

²⁵ 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>.

While Local Law 3 of 2021 was a modest first step in addressing use of biometric technologies by businesses, it was nowhere near sufficient. That law merely requires certain “commercial establishments” that collect, use, or retain “biometric identifier information” from their customers to post signs at all entrances. The minimal notice does not include any information about the specific biometric surveillance tools in use or the collected data and further does not require businesses to disclose for what purpose the technology is used, for how long data is retained, with whom data is shared, or how it is secured. The NYCLU has repeatedly testified on this issue at the committee hearing on October 7, 2019, the hearing by the Department of Consumer and Worker Protection on the proposed rules on August 30, 2021, and the Committee on Consumer and Worker Protection on February 24, 2023. In addition to its important ban on the use of biometric recognition technologies in places of public accommodations, Introduction 217 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 proposed text still defines “biometric identifier information” with respect to information that is “used by or on behalf of a commercial establishment.” The bill, however, would remove the definition of the term “commercial establishment” from the statute. We therefore suggest removing “by or on behalf of a commercial establishment” in order to ensure conformity with the surrounding language.

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

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

Finally, Section 22-1203 amends the existing private right of action of Local Law 3, which requires prior notice of at least 30 days to violating entities, allowing them to cure the violation within 30 days to prevent further action. Although the amendment ensures that an aggrieved person would not have to provide such notice prior to commencing an action against a place or provider of public accommodation that uses a prohibited biometric recognition technology or that shares, sells, or discloses biometric identifier information, the legislation would require those who have been subject to unconsented biometric data collection to first inform violating

entities and allow them 30 days to cure the violation. Such an obligation severely undermines the proposed affirmative written consent protection. The importance of a robust private right of action as an accountability and enforcement tool cannot be overstated, and we strongly urge the Council to strengthen this section to protect against violations.

The NYCLU supports this legislation and urges its passage.

Introduction 425-2024 - Limiting the use of facial recognition technology in residential buildings.

Intro. 425 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.

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

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

Conclusion

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

speech rights. The NYCLU supports Introductions 217-2024 and 425-2024 and we urge their swift passage.



Testimony of the Partnership for New York City

New York City Council Committee on Technology

Int. 217-2024

June 4, 2024

Thank you, Chair Gutiérrez and members of the committee, for the opportunity to testify on Int. 217 which would prohibit places or providers of public accommodation from using biometric recognition technology and protect any biometric identifier information collected. The Partnership for New York City represents the city's business leaders and largest employers. Our members employ 500,000 people in the city and deliver approximately \$200 billion in economic output. We work with government, labor, and the nonprofit sector to promote economic growth and maintain the city's prominence as a global center of economic opportunity, upward mobility, and innovation.

The Partnership supports sensible safeguards for consumers around the use of biometric information but opposes Int. 217 as currently drafted. The proposed legislation would prevent consumers from accessing the substantial benefits of biometric recognition technology. Companies use biometric recognition technology to protect consumers' information, funds, and services. Many customers do not take sufficient measures to protect themselves. For example, they use weak passwords or the same passwords for multiple accounts. Biometric identifiers are a more secure form of protection since they cannot be lost or forgotten and are substantially more difficult to steal than a password. They also help companies prevent fraud and waste by employees.

Biometric recognition technology is also a faster way of authenticating a customer, making security screenings easier and quicker in a variety of high-volume locations such as airports and event venues. Customers make informed choices to use these programs for a more seamless experience. Int. 217 would prohibit these programs.

To allow companies to properly protect consumers and enable consumers to take advantage of the benefits of biometric recognition technology, the Partnership recommends the following changes to Int. 217:

- **Exempt security uses of biometric recognition technology from the ban.** The current bill does not differentiate between different types of uses for this technology. Biometric recognition technology helps protect consumers from fraud and their own mistakes. Washington's law regulating this technology includes an exemption for uses related to a "security purpose" as differentiated from a "commercial purpose." Consumers are required to opt in for commercial uses.

- **Financial firms should be exempt from the proposed law, as they are from current law.** The financial industry was exempted from the current law requiring disclosure of the collection of biometric identifiers by certain businesses because of the high levels of risk in financial transactions and the amount of security required to mitigate such risk. The use and protection of personal information by these firms are already heavily regulated by multiple levels of government. Financial institutions are broadly exempt in both Illinois' and Washington's laws governing biometric recognition technology.
- **Consumers should be permitted to opt-in to using a service that relies on biometric recognition technology.** Int. 217 appears to prohibit voluntary uses of biometric technology (where a customer chooses to use a technology offered by a place of public accommodation for the convenience of the customer). These services already provide a high level of convenience for informed consumers in airports, stadia, etc.
- **The bill should clarify that its provisions apply to consumers and not to employees.** The current law requiring disclosure of the collection of biometric identifier information applies only to customers. The language of the new bill clearly applies to customers in some places and does not specify in other places. Biometric recognition technologies are used by employers to increase security of information and facilities and to prevent fraud. They are also critical for regulatory compliance in certain industries, such as finance.

Attached to this testimony is a list of additional changes we hope you will consider making to the proposed law.

The Partnership is committed to working with the City Council to ensure that individuals' information receives the highest level of protection while also allowing them to benefit from the security and convenience available through new technologies.

Thank you.

Additional Suggested Changes to Int. 217

- Make new language consistent with the current law's focus on actual use in the definition of "biometric identifier information." The definition language in (v) refers to an "identifying characteristic that can be used" (emphasis added). This is inconsistent with the earlier part of the definition (in existing law) that refers to a "characteristic that is used" (emphasis added). (§22-1201)
- Clarify that "Place or provider of public accommodation" refers to physical locations. The current definition is not specific. It would be overly broad to apply the proposed rules limiting the use of biometric recognition technology to online or telecommunications services of companies or consumers who have a nexus to New York City. (§22-1201)
- Ensure that only biometric identifiers obtained through technological means are covered under the law. The requirements to obtain written consent before collection (§22-1202(a)), to develop written policies and safeguards (§22-1202(d), (e)) and to offer a customer the right to have their information erased (§22-1202(f)) appear to apply to information not obtained through technological means. These could apply to easily observable characteristics such as height, gender, hair and eye color, etc. This seems overbroad when divorced from a technological method of detection or collection.
- Allow a place or provider of public accommodation the option to notify customers directly about biometric data collection and use instead of posting a sign. Customers may not notice the sign currently required and such sign may not provide as much information as an employee. The customer would also be more likely to ask questions if provided information directly from an employee. (§22-1202(a))
- Allow a place or provider of public accommodation to rely on a vendor to assess "risks in network and software design". An entity that relies on a vendor for its biometric information technology should be able to rely on the vendor's representations about risks because the vendor would not likely reveal its source code to the entity, making an assessment of software design impossible. (§22-1202(e))
- Ensure the law exempts traditional security measures and information that is not analyzed with technological means or sold to third parties. (§22-1201 & §22-1204)
 - There is some confusion about whether the definition of "Biometric recognition technology" captures traditional physical security measures (e.g., cameras). This is further complicated by the removal of the exemption from the current law's disclosure requirements for "information collected through photographs or video recordings, if: (i) the images or videos collected are not analyzed by software or applications that identify, or that assist with the identification of, individuals based on physiological or biological characteristics, and (ii) the images or video are not shared with, sold or leased to third-parties other than law enforcement agencies."
 - This could be clarified by explicitly exempting information collected through photographs, video and audio where that information is not analyzed by software or applications that identify individuals based on physiological or biological characteristics.

- Clarify the financial institution exemption in §22-1204(i).
 - Many financial institutions are subject to the Interagency Guidelines Establishing Information Security Standards (promulgated by Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation). These rules are included in the Code of Federal Regulations, but it is unclear whether the reference to “regulations” in §22-1204 is intended to capture the guidelines.
 - The regulations (or guidance) under Title V of the Financial Services Modernization Act of 1999 apply only to “customer information” and thus would exclude activities that occur before a financial institution establishes a continuing relationship with an individual as well as business to business activities.
- Add an exemption for disclosures of biometric information that are required by law or court order.



**Testimony on Behalf of the Retail Council of New York State
Regarding Introduction 217-2024**

**New York City Council Committee on Technology
June 10, 2024**

Testimony submitted by:
Kelsey Dorado Bobersky
Director of State and Local Government Relations
Retail Council of New York State
kelseydorado@rcnys.com

Chair Gutiérrez and Honorable Committee Members:

Good afternoon. My name is Kelsey Dorado Bobersky; I am the Director of State and Local Government Relations for the Retail Council of New York State. Our organization is the state's leading trade group for the retail industry, representing member stores in New York City and across the state, ranging from the smallest independent merchants to national and international brands. Thank you for the opportunity to speak today on Introduction 217-2024.

As currently drafted, the captioned legislation would prohibit “any place or provider of public accommodation to use any biometric recognition technology to verify or identify a customer” and require covered entities, including retail stores, to “get the written consent of such customer in advance of any collection.”

On behalf of independent stores and national brands throughout the five boroughs, we are opposed to the provisions outlined in the bill.

Specifically, the requirement that stores obtain written consent of “such customer in advance of any collection” is impractical, as it would require merchants with basic-model video or photo cameras to obtain written consent of each customer before they entered the store. This would completely disrupt the flow of commerce in a city that is often referred to as the retail capital of the world.

In addition, the bill would effectively prohibit stores in New York City from using certain technology to address organized retail crime incidents and habitual retail theft, as it does not exempt the use of biometric technology used solely for fraud prevention or security purposes. This prohibition is something we oppose outright, due to our ongoing efforts to promote store and community safety in neighborhoods throughout the state.

For context, the Retail Council of New York State continues to prioritize the safety of employees and customers, as we have done for the last several years. We participate in the mayor's Retail Theft Task Force and strongly support the retail theft prevention initiatives included in the FY 2024-25 State Budget, including:

- Interagency coordination at the state and local level – and related funding.
- Dedicated prosecutors in district attorney offices for cases involving retail theft, along with funding for implementation.
- Allocation of funding to “deploy a dedicated State Police team to build cases against organized retail theft rings and create a new State Police enforcement unit dedicated to this purpose.”
- Allocation of state funding to “build the capacity of local law enforcement efforts to combat retail theft.”
- Increased penalties for the assault of retail workers.
- Creation of a “commercial security tax credit” for small businesses.

This is a real and significant issue that must be addressed in a strategic manner. As such, we urge the City Council to exempt the use of biometric technology for security purposes, as this information is critical to address public safety matters in store settings throughout the city.

Finally, we oppose the provision that would establish a private right of action. The requirements in the bill would apply to stores that invest in New York City, and it is important to note that they are in constant competition with online companies that choose not to open a storefront in the five boroughs. Expressly authorizing expensive lawsuits against New York brands would effectively provide online companies with yet another competitive advantage over brick-and-mortar retail.

We pledge to remain constructive as your committee considers issues related to retailers in New York. However, we oppose this bill in its current form.

Respectfully submitted,

Kelsey Dorado Bobersky
Director of State and Local Government Relations
Retail Council of New York State
kelsydorado@rcnys.com



June 10, 2024

The Honorable Jennifer Gutiérrez
Chair
Committee on Technology
New York City Council
New York, NY

Written Testimony of SIA for Committee on Technology Hearing, “Oversight – Cybersecurity of New York City Agencies”

Dear Chair Gutiérrez 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 1,500 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. While we support policies that would help ensure responsible and effective use of such technologies,¹ we have serious concerns with the two proposals relating to biometric technologies being discussed at today’s hearing, Int. No. 217-2024 (Hanif)² and Int. No. 425-2024 (Rivera).³

Blanket Ban on use of Biometric Technologies by Businesses, Customers

As drafted, Int. No. 217 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 For example, SIA has published its *Principles for the Responsible and Effective Use of Facial Recognition* -

<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=6557556&GUID=E67A1D7D-5245-4373-B5FF-1AD968E3383F&Options=&Search=>

³ <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=6558031&GUID=73676D60-2010-4A95-AB2F-A0B96A46C45E&Options=&Search=>

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 authorized in the underlying law over such a sweeping prohibition, as biometric technologies are 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).

We know this because of the of 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.⁴

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 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

⁴ <https://progresschamber.org/wp-content/uploads/2023/03/Who-Benefits-from-BIPA-Analysis-of-Cases-Under-IL-Biometrics-Law.pdf>

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 address the current crisis of organized retail crime, in conflict with Mayor Adams’ initiatives to fight retail crime and his encouragement and assistance to local businesses to “analyze and improve their security.”⁵ According to the Mayor, 25,480 arrests for retail theft were made in in 2023 alone, and 30% involved just 542 repeat offenders.⁶ And according to a City report, as of last year retail theft in New York City had risen nearly 80% since 2018.⁷

While retailers across the state are losing over \$4 billion annually to such theft⁸ the human cost to such crimes is critical to understand and address. Retail crime is often violent crime, it’s not just “shoplifting.” Over the last two years, more than 1,100 customers, employees, and security personnel have been killed by criminals in retail settings.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.

Biometrically enabled security systems have become a key technology tool for fighting organized retail crime. Such technologies leveraging facial recognition software are used by stores daily across New York City and the nation to help address this crisis and increasingly to make stores safer. There are many examples of the types of daily success achieved in preventing theft as well as violence against employees using these technologies,¹⁰ 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 are able to 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.¹¹ 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.¹²

Nevertheless, the proposed Int. No. 217 would outright ban use of these critical technology tools, despite the benefits and the fact that the City’s existing biometric data privacy law¹³ already regulates the use of such systems.

⁵ Mayor’s remarks - <https://www.nyc.gov/office-of-the-mayor/news/383-24/mayor-adams-new-pilot-program-combat-retail-theft-create-efficiencies-improve#/>

⁶ Ibid.

⁷ <https://www.nyc.gov/assets/home/downloads/pdf/office-of-the-mayor/2023/combating-retail-theft-report-may-17-2023.pdf>

⁸ <https://nypost.com/2023/11/26/business/ny-retailers-blast-hochul-over-theft-which-has-cost-stores-4-4-billion/>

⁹ Analysis of data and reports from Downing & Downing, Inc, see <http://d-ddaily.com/archivesdaily/2023-Q4-Fatalities-Report.htm>.

¹⁰ <https://losspreventionmedia.com/face-matching-leads-to-big-wins-for-retailers/>.

¹¹ Ibid.

¹² <https://www.securityindustry.org/report/u-s-public-opinion-research-on-the-support-of-facial-recognition/>

¹³ <https://codelibrary.amlegal.com/codes/newyorkcity/latest/NYAdmin/0-0-0-42626>

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

Similar to the impact of Int. No. 217 on commercial and consumer applications, Int. No. 425 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 tenant use must be voluntary.¹⁴

Instead of 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 numbers, etc) and addressing the risk of keys, cards or fobs being lost, stolen or misused. Enactment of this proposal would preclude residents from such options to use more secure, convenient and technologically advanced methods of authentication and access, which may in fact be among benefits guaranteed in existing rental agreements.

Breaking Down Biometric "Myths"

Unfounded claims regarding increased risk of misuse or compromise with respect to biometric information and the accuracy of facial recognition technology have often driven calls for bans. Addressed below are the three most common myths.

- **Myth 1:** *If my biometrics are compromised, I'll lose my identity.* Modern biometric identification technologies generate and use abstract numerical representations made by deep-learning models, not our actual "features." This data is created and readable only within the specific proprietary software used and is "matched" based on the mathematical similarity between enrolled and comparison information. This makes biometric data irreversible (cannot be reverse engineered to reveal the image or feature measured), incompatible with other systems and unusable by third parties. 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.
- **Myth 2:** *Passwords can be reset, biometrics can't.* Even in the unlikely event of a breach into a biometric database (from which the data would be unusable due to its nature), operators can swiftly respond by simply updating to a new software version or encrypting the data with a new key. Biometric data for the same individual is also infinitely changeable in that it will be slightly different each time it is created by the software (due to varying positions of a finger placed on a sensor or

¹⁴ <https://www.nyc.gov/site/hpd/services-and-information/tenant-data-privacy-law.page>.

varying photography conditions for example) for enrollment or comparison. This data can easily be “reset” as needed.

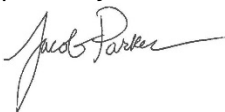
- **Myth 3:** *Facial recognition technology is plagued by race, gender, and age bias.* While there is evidence that some early versions struggled to perform consistently across various demographic factors, modern technologies exhibit minimal “bias.” Most providers are evaluated by the U.S. government’s National Institute of Standards and Technology (NIST) on an ongoing basis. For over 20 years, the NIST Face Recognition Technology Evaluation (FRTE) Program has remained the world standard for objective, third-party scientific evaluation, providing an “apples to apples” comparison of the performance of facial recognition technologies.

This U.S. government 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**. And according to one of the latest FRTE evaluations using race-labeled images, **the top 100 are over 99.5% accurate in matching images across Black male, white male, Black female and white female demographics**. For the top 60 of these, accuracy for the highest performing demographic versus the lowest varies only between 99.7% and 99.85%. And unexpectedly, white male is the lowest performing of the four demographic groups among these top technologies.¹⁵

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

¹⁵ See analysis of accuracy claims and of NIST data - <https://www.securityindustry.org/2022/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/>



40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (212) 518-7573

**STATEMENT OF
NINA LOSHKAJIAN, STAFF ATTORNEY
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT (“S.T.O.P.”)**

**BEFORE THE COMMITTEE ON TECHNOLOGY,
NEW YORK CITY COUNCIL**

**SUPPORTING THE PASSAGE OF
INTRODUCTIONS 217-2024 AND 425-2024**

**PRESENTED
June 10, 2024**

Good morning, Chair Gutiérrez, and members of the Committee on Technology. Thank you for organizing this important hearing. We appreciate the opportunity to testify today on the harms of biometric surveillance. The Surveillance Technology Oversight Project (“S.T.O.P.”) is a New York-based civil rights and anti-surveillance group. S.T.O.P. advocates and litigates against discriminatory surveillance.

We urge the Council to pass Intros 217-2024 and 425-2024, banning public accommodations and landlords, respectively, from using facial recognition and other biometric tracking tools. Biometric tracking, including facial recognition, is biased, error-prone, and harmful to marginalized communities. It’s illegal for stores and landlords to discriminate on the basis of race, so why do we let them use racist technology? Simply put, these systems have no place in New York City’s stores and homes. These measures are an indispensable safeguard for New Yorkers, but we also implore the Council to go farther and introduce legislation banning law enforcement and government abuse of this dangerous technology.

I. The Harms and Bias of Biometric Surveillance

Facial recognition’s proliferation across our city is creating a bleak dystopia in which New Yorkers are watched wherever they go, posing particular risks to Black, Latinx, and non-binary and transgender New Yorkers of harassment, exclusion, and wrongful arrest. The Council must act to protect our civil liberties and our freedom of movement.

Facial recognition has been proven time and time again to be racially biased, with higher rates of inaccuracy on people of color. These systems can be up to 99% accurate for middle-aged white men under ideal lighting in laboratory conditions but can be wrong more than 1 in 3 times for some women of color, even under similar conditions.¹ The same exact software, the same exact hardware—but dramatically different outcomes for Black and brown New Yorkers. Every publicly reported case of an individual wrongly arrested after being misidentified through facial recognition has involved a Black person.²

Similarly to how the technology has not been sufficiently trained to differentiate between faces of color, it has also been designed to assign each face a specific gender—male or female—and cannot recognize anything else. This leaves transgender and non-binary individuals susceptible to misidentification and wrongful arrest.³ People will also be excluded from partaking in society freely. Just last week it was reported that a new dating app for lesbians, L’app, would use facial recognition

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

² 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>; Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men’s Lives*, WIRED, March 7, 2022, <https://www.wired.com/story/wrongful-arrests-aiderailed-3-mens-lives/>; Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES, Dec. 29, 2020, <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>.

³ Rachel Mentz, *AI Software Defines People as Male or Female. That’s a Problem*, CNN BUSINESS, Nov. 21, 2019, <https://www.cnn.com/2019/11/21/tech/ai-gender-recognition-problem/index.html>.

to ban trans women from creating profiles.⁴ Immigrants suffer as well. A biometric scanning feature on a Customs and Border Protection (CBP) app failed to accept photos of dark-skinned African and Haitian migrants applying for asylum.⁵

Even if the algorithms could be improved, biometric tracking systems would remain just as discriminatory because of the ways they are plugged into discriminatory policing, housing, and commercial practices. BIPOC tenants and shoppers will not be given the same benefit of the doubt as white tenants and shoppers when faced with a facial recognition error. There can be no truly neutral technology, so there is no technical fix for facial recognition's bias.⁶ For example, facial recognition searches are skewed by where surveillance cameras are placed in our city. The technology is misused in a way that further replicates historical biased policing, with disproportionately high placement of cameras in low-income communities of color.⁷ A recent analysis by Amnesty International found that "areas across all boroughs with higher incidents of stop-and-frisk are also areas with the greatest current exposure to facial recognition," and further, "the higher the proportion of non-white residents, the higher the concentration of facial recognition compatible CCTV cameras."⁸

Allowing businesses and landlords to collect and store biometric information also poses unique security risks given the sensitivity of the data, making these entities an extremely lucrative target for identity thieves and hackers.⁹ Biometric identifiers are frequently used for ID verification and allocating public benefits; this makes an individual's biometric information an attractive target for fraudsters, as hackers can, and do use biometric identifiers to access computer systems.¹⁰ More dangerous than other personal identifiers like a social security number, biometric identifiers are static and are almost impossible to change.¹¹ When a hacker acquires another person's biometric data, it puts them at risk for identity theft for the rest of their lives.¹² Last month, Outabox, an

⁴ Mathew Rodriguez, *Anti-Trans Advocate's Lesbian Dating App Uses Facial Recognition to Exclude Trans Women*, THEM, June 3, 2024, <https://www.them.us/story/anti-trans-lesbian-dating-app-lapp-facial-recognition>.

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

⁶ *See How Emerging Technologies Amplify Racism—Even When They're Intended to Be Neutral*, CBC RADIO, June 19, 2020, <https://www.cbc.ca/radio/spark/we-behave-differently-if-we-know-we-re-being-watched-1.5619106/how-emerging-technologies-amplify-racism-even-when-they-re-intended-to-be-neutral-1.5619107>.

⁷ Eleni Manis et al., *Scan City: A Decade of NYPD Facial Recognition Abuse* (Surveillance Technology Oversight Project, July 8, 2018).

⁸ *Inside the NYPD's Surveillance Machine*, AMNESTY INTERNATIONAL, <https://banthescan.amnesty.org/decode>.

⁹ *US Government Hack Stole Fingerprints of 5.6 Million Federal Employees*, THE GUARDIAN, Sept. 23, 2015, <https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints>. Dan Rafter, *Biometrics and Biometric Data: What Is It and Is It Secure?*, NORTON, May 6, 2022, <https://us.norton.com/blog/iot/what-is-biometrics>.

¹⁰ A. Dellinger, *Hackers Defeat Vein Authentication by Making a Fake Hand*, ENGADGET, Dec. 28, 2018, <https://www.engadget.com/2018-12-28-hackers-defeat-vein-authentication-by-making-a-fake-hand.html>.

¹¹ Anthony Ortega, *Do Biometrics Protect Your Data or Put Your Identity at Risk?*, SPICEWORKS, Oct. 8, 2018, <https://www.spiceworks.com/it-security/data-security/articles/do-biometrics-protect-your-data-or-put-your-identity-at-risk/>.

¹² *Is Your Identity at Risk from Biometric Data Collection?*, BeyondTrust (last accessed Oct. 6, 2022), <https://www.beyondtrust.com/blog/entry/is-your-identity-at-risk-from-biometric-data-collection>.

Australian firm that produces facial recognition used for entry to bars and clubs, suffered a massive breach, jeopardizing the personal information of millions of people.¹³

II. Intro 217

New Yorkers should not be forced to accept constant tracking as part of simple activities like buying groceries or taking their kids to a baseball game. Stores' biased facial recognition systems will exclude Black and dark-skinned people due to incredibly common mismatches. Police will be called on innocent people, which will result in dangerous encounters and potentially unnecessary racialized violence. Facial recognition expansion threatens interstate abortion-seekers, people seeking gender-affirming care, and undocumented immigrants, simply because they enter a store. Yet facial recognition use in public spaces is on the rise across New York City. In 2022, the Mets implemented a facial recognition ticketing system at Citi Field.¹⁴ In partnership with Wicket, a computer vision company, the Mets are encouraging fans to upload selfies on MLB.com to register their faces and then check-in at the gates. The Mets have touted this system as a new high-tech amenity. But facial recognition is not an amenity, it is discriminatory surveillance. And it is far from high-tech, as it often struggles to identify faces when people are wearing hats, seemingly an obvious issue for fans headed to a baseball game.¹⁵

James Dolan, the owner of Madison Square Garden Entertainment Corporation (MSG), has faced scrutiny for his use of facial recognition at the company's venues, including from New York State Senators¹⁶ and Attorney General James.¹⁷ Dolan has used the invasive power of the technology to seek vengeance against MSG's foes, blocking access to ticketholders who are affiliated with law firms involved in pending lawsuits against MSG. In one case, this meant ejecting a mother trying to watch the Rockettes show at Radio City Music Hall with her daughter's Girl Scouts troop.¹⁸ Business owners, especially wealthy, celebrity business owners, should not be allowed to use such dangerous tech to follow their whims or punish anyone who displeases them.

Facial recognition is already used in some grocery stores, like Fairway Market, which is scanning the face of every single customer walking through their stores and storing that sensitive personal

¹³ Jordan Pearson, *The Breach of a Face Recognition Firm Reveals a Hidden Danger of Biometrics*, WIRED, May 2, 2024, https://www.wired.com/story/outabox-facial-recognition-breach/?utm_source=substack&utm_medium=email.

¹⁴ 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.sportstechie.com/the-new-face-of-baseball-mets-to-roll-out-facial-recognition-ticketing-at-citi-field>.

¹⁵ Sam Van Doran and David Siffert, *The Mets Should Steal Bases, Not Faces*, N.Y. DAILY NEWS, Sept. 15, 2022, <https://www.nydailynews.com/opinion/ny-oped-bases-not-faces-mets-20220915-cuuul25jjnh5rbzbbsvmrbwauy-story.html>.

¹⁶ [Albany takes on attorney ban at Madison Square Garden \(ny1.com\)](https://www.albany.gov/newsroom/press-releases/albany-takes-on-attorney-ban-at-madison-square-garden-ny1-com)

¹⁷ Andrea Vittorio, *Madison Square Garden Pressed by NY AG James Over Face Scans*, BLOOMBERG LAW, Jan. 25, 2023, <https://news.bloomberglaw.com/privacy-and-data-security/madison-square-garden-pressed-by-ny-ag-james-over-face-scans>.

¹⁸ Sarah Wallace, *Face Recognition Tech Gets Girl Scout Mom Booted From Rockettes Show — Due to Where She Works*, NBC N.Y., Dec. 19, 2022, <https://www.nbcnewyork.com/investigations/face-recognition-tech-gets-girl-scout-mom-booted-from-rockettes-show-due-to-her-employer/4004677/>

data indefinitely.¹⁹ The Federal Trade Commission (FTC) has recognized how dangerous it is when stores use this technology irresponsibly, recently banning Rite Aid from using facial recognition for five years.²⁰ The FTC complaint against Rite Aid charged that the company did not take reasonable measures to prevent harm to its customers, leading to wrongful accusations of shoplifting by employees because the algorithm had falsely flagged a face as a match for a previously identified shoplifter.²¹

Intro 217 specifically prohibits any place or provider of public accommodation from using any biometric recognition technology to verify or identify a customer. It also prohibits businesses from barring entry to customers based on biometric recognition technology and prevents companies from selling customers biometric data. This would be a crucial step towards protecting New Yorkers and preventing the types of abuses of the technology that we are seeing in places of public accommodation like MSG.

III. Intro 425

Facial recognition has no place in our homes. This technology opens tenants and their guests to harassment and discriminatory eviction or exclusion from their homes, and it compromises their privacy. Without legal intervention, collection of biometric data can be forced upon not just all residents, but any guests they have over as well, with Black, brown, Asian, and gender non-conforming guests barred from visiting their friends due to facial recognition mismatches. In New York City public housing, facial recognition use has already led to residents being evicted for minor violations of policy, contributing to the massive eviction crisis.²² Banning facial recognition in residences is essential to safeguard New Yorkers from losing their homes or their ability to fully enjoy their rights as tenants.

It cannot be overemphasized just how much detailed information biometric tracking gives landlords about our lives: our schedules and routines, who our romantic partners and friends are, what hours we get home. It allows landlords to monitor our movements on a previously unfathomable scale. You can give any friend your key code or access fob, but you can't give them your face. Proponents of biometric entry systems have not been shy about their ambitions to collect as much personal information as possible. Take, for example, the disclaimer on the website of one vendor, GateGuard, which scarily warns customers: "You should understand even if you opt-out of using face recognition instead of an ID number, your building may still have the legal right to

¹⁹ Lynda Baquero, *Your NYC Supermarket May Know Your Face Better Than You Think*, NBC NEWS, March 15, 2023, <https://www.nbcnewyork.com/news/local/nyc-supermarket-uses-face-recognition-software-but-why-and-where-the-info-going/4157198/>.

²⁰ 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/pressreleases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without>.

²¹ *Id.*

²² 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>.

film, record, and recognize those who come into the building.”²³ Ari Teman, the founder and CEO of GateGuard, has proudly touted how GateGuard’s systems can be used to “catch” tenants with unlisted roommates, a cruel proposition given the reality of how many New Yorkers struggle to make rent payments and rely on roommates to do so.²⁴

New Yorkers do not want this invasive technology used in their homes, the most intimate of spaces. In 2019, the tenants of Atlantic Plaza Towers in Brooklyn organized in response to their landlord’s attempted installation of a facial recognition entry system and successfully prevented the plan from proceeding.²⁵ Their organizing highlighted the disproportionate impact of the use of these biometric security systems in low-income communities of color.²⁶

The racial bias of facial recognition will inevitably inconvenience residents in accessing their home and may even elicit an unwarranted law enforcement response. Further, New York City landlords have been accused of sharing tenants’ most sensitive information—phone numbers, photos, and even Social Security numbers—with immigration officials.²⁷ To protect immigrant communities in our city, we cannot let landlords have access to residents’ biometric data.

Intro 425 would prohibit any owner of a multiple dwelling from installing, activating, or using any biometric recognition technology that identifies tenants or the guest of a tenant. One important addition should be made to the bill: a strong private right of action that would give tenants and their guests a way to hold landlords accountable. This should be applicable to all provisions, not just sale, and allow for statutory damages and punitive damages. Passage of this bill is critically important to make New Yorkers safer in their homes and to not contribute further to our city’s housing crisis.

IV. The Need for Additional Legislation

While we are heartened to see the introduction of these two bills, we are disheartened that the Council has still not directly addressed the growing threat of how this biased and dangerous tool is used by police. We applaud the Council for paying attention to the issue of use in businesses and in residential settings, but legislation banning its use by government agencies is necessary to meaningfully protect New Yorkers from harm. It’s been over a year since S.T.O.P. drafted legislation for the Council to ban police use of biometric surveillance technology, but the Council has not even introduced a bill yet or included it on any committee agenda.

²³ Alfred Ng, *Smart Home Tech Can Help Evict Renters, Surveillance Company Tells Landlords*, CNET, Oct. 25, 2019, <https://www.cnet.com/home/smart-home/install-smart-home-tech-evict-renters-surveillance-company-tells-landlords>.

²⁴ *Id.*

²⁵ Yasmin Gagne, *How We Fought Our Landlord’s Secretive Plan for Facial Recognition—and Won*, Nov. 22, 2019, FAST COMPANY, <https://www.fastcompany.com/90431686/our-landlord-wants-to-install-facial-recognition-in-our-homes-but-were-fighting-back>.

²⁶ *Id.*

²⁷ See, e.g., Lauren Cook, *Queens Landlord Gave Tenant Information to ICE After Discrimination Complaint, Commission Says*, N.Y. DAILY NEWS, July 19, 2017, <https://www.amny.com/news/queens-landlord-gave-tenant-information-to-ice-after-discrimination-complaint-commission-says-1.13810387>.

The New York City Police Department (NYPD) is already engaged in biometric surveillance at a massive scale: the Domain Awareness System includes an inter-connected network of over eighteen thousand surveillance cameras.²⁸ Officers reported in open-records litigation that the department used facial recognition technology more than 22,000 times in just three years.²⁹ S.T.O.P. has been litigating for four years to get the most basic info from NYPD on the bias and accuracy of its use of facial recognition.³⁰

This is an urgent issue. People's lives are being ruined by police use and misuse of facial recognition. 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 recognition and falsely accused of robbery and carjacking.³¹ Her time in jail caused serious medical complications, including contractions and sharp pain, leading her to be hospitalized immediately upon release. There are multiple similarly heartbreaking stories; three Black fathers, two also in Detroit and one in New Jersey, were wrongfully arrested and jailed following faulty facial recognition matches, and these cases each had devastating lasting consequences.³² In one particularly worrisome case, a black man was wrongfully arrested in Georgia for a crime committed in Louisiana and spent six days in jail, despite the fact that he had never been to Louisiana.³³

Officers use pseudoscientific tactics that exacerbate the risk of error, such as running scans of celebrity lookalikes.³⁴ The Georgetown Law Center on Privacy and Technology documented the kinds of abuses that are “common practice” at NYPD.³⁵ One of the most egregious practices is that of routinely altering photos. The report revealed that NYPD edits of images “often go well beyond minor lighting adjustments and color correction,” and in many instances “amount to fabricating completely new identity points not present in the original photo.”³⁶

Police also abuse this dangerous technology to surveil protestors. There are reports that the NYPD used facial recognition to target Derrick Ingram for his leadership of a peaceful Black Lives Matter

²⁸ Rocco Parascandola, *New NYPD Surveillance Cameras to Cover Stretch of Upper East Side Not Easily Reached by Patrol Cars*, NY Daily News, Oct. 23, 2019, <https://www.nydailynews.com/2018/10/24/new-nypd-surveillance-cameras-to-cover-stretch-of-upper-east-side-not-easily-reached-by-patrol-cars>.

²⁹ <https://www.stopspying.org/latest-news/2020/10/23/stop-condemns-nypd-for-22k-facial-recognition-searches>.

³⁰ <https://www.stopspying.org/nypd-facial-rec-bias>.

³¹ 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>.

³² Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*, WIRED, March 7, 2022, <https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/>.

³³ 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-lawsuitsb613161c56472459df683f54320d08a7>.

³⁴ 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>.

³⁵ 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 *Id.*

protest. Police later surrounded Derrick's home with more than 50 officers as part of a retaliatory raid.³⁷

We call on the Council to introduce legislation banning all government use of facial recognition. In continuing to fail to act to ban the technology, New York falls further and further behind progressive cities from around the world.³⁸ Because of its documented biases and its replication of historically flawed police practices, facial recognition should not be used by the NYPD or any other government agency.

Thank you for the opportunity to testify today.

³⁷ 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>.

³⁸ Shannon Flynn, *13 Cities Where Police Are Banned from Using Facial Recognition Tech*, INNOVATION & TECH TODAY, Nov. 18, 2020, <https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech>; Kyle Wiggers, *AI Weekly: EU Facial Recognition Ban Highlights Need for U.S. Legislation*, VENTUREBEAT, Oct. 8, 2021, <https://venturebeat.com/2021/10/08/ai-weekly-eu-facial-recognition-ban-highlights-need-for-u-s-legislation>.



Paul Zuber
Executive Vice President

June 11, 2024

Hon. Jennifer Gutiérrez
Chair, Committee on Technology
The New York City Council
City Hall
New York, NY 10007

Dear Chair Gutiérrez,

I am writing on behalf of The Business Council of New York State, New York's largest statewide business association, and our 3,200 business members, to express our strong concern with proposed legislation that would prohibit the use of biometric identification technologies (BID). We believe that New York City Council Bill, Intro no. 0425, however well-intentioned, would have a negative impact on consumers and businesses.

The Business Council has the benefit of representing a wide array of businesses. Our members are part of every sector of the New York state economy. Our members also operate businesses throughout the state, with many of our members operating businesses within the City of New York. Our broad-reaching membership gives us a unique opportunity to understand how legislation, and in particular this legislation, will impact businesses both large and small operating in New York City.

This proposal would outlaw nearly all uses of BID technologies by businesses in interactions with customers and employees regardless of the purpose or whether it is an integral part of a service requested or agreed to by the customer. In addition, the proposal would result in the loss of the significant amount of money (and time) already invested in BID hardware and software by NYC businesses and would require the replacement of that equipment and all associated costs. This would force businesses which already use BID technologies to scramble for an equivalent substitute. That substitute will depend on whether a viable one even exists. Since the bill would expand the definition of "biometric identifier information" to include any identifying characteristic that can be used "in combination...with other information" to establish individual identity, the bill would cover a wide range of non-biometric information that is commonly accepted, such as: photos and video from security cameras that include images of objects and people. This would only place an enormous burden on consumers and businesses.

The fact is that, in society, there is a place for BID technologies, and it is something that consumers want from the businesses they frequent. There are numerous examples of how BID technology benefits most New Yorkers. These include:

- o Secure building and door access control systems for workers
- o Authenticated app-based accounts and payment systems, both online and in-person
- o A more convenient form of payment and access at sporting and other entertainment venues
- o Fingerprint time-clocks and cash register locks by business employees
- o Driver authentication for ride-share services
- o Security systems protecting persons or property, including systems augmenting loss prevention efforts
- o Streamlined embarkation on cruise ships and seamless “curb-to-gate” air travel

Finally, this bill would place enormous burdens related to data retention, destruction, security, risk assessment, control system monitoring, etc. on any New York businesses that collect the BID info “of any person.” “Any person” is not limited to customers or even persons in New York City and appears to apply to employees as well.

In the end, this legislation will not just further burden businesses, but ultimately it will hurt the consumers in which the bill purportedly wants to protect. Although we are sure there are valid and good intentions behind the bill, this legislation simply does not help New Yorkers and places more of a burden on doing business in New York City.

Thank you for the opportunity to comment.

Sincerely,

A handwritten signature in black ink, appearing to read "Paul Zuber". The signature is fluid and cursive, with a large initial "P" and "Z".

Paul Zuber
Executive Vice President
The Business Council of New York State, Inc.

THE LEGAL AID SOCIETY

Justice in Every Borough.

TESTIMONY

The Council of the City of New York
Committee on Technology

An oversight hearing on the Cybersecurity of New York City Agencies

June 10, 2024

The Legal Aid Society
199 Water Street
New York, NY 10038

By: Shane Ferro
Digital Forensics Unit
Staff Attorney
(718) 286-2071
SFerro@legal-aid.org

Good morning. I am Shane Ferro, a Staff Attorney for The Legal Aid Society's Digital Forensics Unit, a specialized unit providing support for digital evidence and electronic surveillance issues for The Legal Aid Society's attorneys and investigators, in all five boroughs. I thank these Committees for the opportunity to provide testimony today on the need to ban the use of facial recognition and other biometric surveillance in residences and public accommodations here in New York City.

I. ORGANIZATIONAL INFORMATION

Since 1876, The Legal Aid Society 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, the Society serves as the primary defender of indigent people prosecuted in the State court system.

In 2013, The Legal Aid Society created the Digital Forensics Unit to serve and support Legal Aid attorneys and investigators in our criminal defense offices. Since that time, we have expanded to two digital forensics facilities, three analysts, two senior analysts, four staff attorneys, one paralegal, and one supervising attorney. Members of the Unit are trained in various forms of digital forensics and have encountered multiple different types of electronic surveillance used by law enforcement.

II. BACKGROUND ON BIOMETRIC SURVEILLANCE AND FACIAL RECOGNITION

Systems or technologies that analyze people's personal, physical identifying information, or biometric data, in public spaces are called biometric mass surveillance. This can be DNA, heart rate, or gait analysis, but is most commonly (in the public surveillance context) facial recognition, because of the proliferation of public and private surveillance cameras in dense

cities such as New York. This testimony focuses on the uses and harms of facial recognition in the context of the two bills being considered today: Intro 217, banning the use of biometric surveillance in public places, and Intro 425, banning the use of facial recognition in residential buildings.

In January 2024, the National Academy of Sciences released a comprehensive report on facial recognition technology, its current and future uses, and the societal harms that its use poses (“NAS Report”).¹ The report states,

[F]rom a societal perspective, FRT is problematic because it impacts a core set of interests related to freedom from state and/or private surveillance, and hence control over personal information. Its use therefore has the ability to interfere with and substantially affect the values embodied in commitments to privacy, civil liberties, and human rights.²

The concerns over widespread use of facial recognition are not theoretical. Extensive use of facial recognition in public in China has led to behavioral engineering—essentially making people so afraid that they can be targeted for public humiliation that they substantially change how they behave, dress, and interact everywhere in public.³ Facial recognition technology can lead to misidentification and specific harms to specific individuals, which this testimony will discuss further, but from a regulatory perspective it is also important to consider the broader societal harm that comes from allowing the technology to proliferate in such a way that their face can be recognized by every surveillance camera they pass, making it not just possible but likely that every person can be tracked throughout the city from camera to camera, not just in special

¹ National Academy of Sciences, “Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance,” January 2024, <https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance>, retrieved June 5, 2024.

² *Id.* at 26-27.

³ Ng, Alfred, “How China uses facial recognition to control human behavior,” CNET, August 11, 2020. <https://www.cnet.com/news/politics/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/>, retrieved June 5, 2024.

extenuating circumstances, but as they go about their day, every day. We are not quite there yet in New York City, but that loss of privacy and autonomy is something that we have to actively work against, or it will take hold here.

Although we call it “facial recognition technology,” this is a misnomer. Recognition is a fundamentally human action. What computers do is find similarities. FRT is actually an algorithm that runs one photo of a face against a dataset (of either one or many faces, depending on the type of system), and measures similarities.⁴ A match is not the same as human recognition, but instead a mathematical determination of similarity. The degree of similarity required to be considered a match is set by either the manufacturer or the end user—with a baked-in assumption that some degree of error is considered acceptable.⁵

False positives (a “match” by the software that identifies the wrong person) are a huge concern and cause the most direct harm to individuals. Racial minorities face higher rates of false positives.⁶ This is not a coincidence. Historic racial bias is baked into how these systems are made. “Many FRT systems deployed in the United States are trained on imbalanced, disproportionately White, data sets.”⁷ Different facial recognition algorithms vary widely in their accuracy, but almost uniformly have been found to be worse at matching Black faces than other racial groups, worse at matching women than men, and worse at matching the old and the young versus middle aged people.⁸ In other words, facial recognition algorithms are most likely to be wrong about the identities of people in a variety of marginalized social groups. Those in

⁴ NAS Report at 47.

⁵ *Id.*

⁶ NAS Report at 82.

⁷ *Id.*

⁸ Grother, Patrick, et al., “Facial Recognition Vendor Test, Part 3: Demographic Effects,” National Institute of Standards and Technology, U.S. Department of Commerce, December 2019, available <https://doi.org/10.6028/NIST.IR.8280>, retrieved June 6, 2024, at 10.

protected classes on the basis of race, gender, and age are the most at risk for individualized harm through the use of these technologies.

Of the known cases of FRT false positives leading to wrongful arrests, all cases but one have involved Black individuals.⁹ However, a false positive does not need to lead to a full loss of liberty to be harmful. Someone could be prevented from shopping in a grocery store, escorted out of a sports arena despite paying for a ticket, or not let into the building of their own home. These more quotidian humiliations could be the result of false positives or could be the system working as designed. However, the harm of these systems is not concentrated in examples of someone refused service or locked out of a building.

There is also harm in the data itself existing. According to the National Academy of Sciences,

In addition to general privacy concerns raised by inclusion in large databases, data in such centralized repositories are highly sensitive and may be an attractive target for exfiltration by third parties, including criminals and foreign governments. Indeed, it is potentially highly useful to adversaries of the United States.¹⁰

Biometric surveillance technologies require access to huge amounts of knowledge about the personal identifying information of thousands, even millions of individuals to run. That data has to be collected and stored, which makes it vulnerable to hacking and theft. At this point, almost every person in the country has been the victim of a password data breach and has had their personal information be vulnerable to attack. With biometric surveillance it is our most personal information that can be commoditized, hacked, and stolen, and, unlike a password, it cannot be easily changed. The only real way to prevent this from happening is to limit the number of these systems that are allowed to be collecting and storing this information in the first place.

⁹ NAS Report at 83.

¹⁰ *Id.* at 89.

III. FACIAL RECOGNITION TECHNOLOGY HAS NO PLACE IN RESIDENCES

Citizens have a right not to be surveilled in their own homes. We know that facial recognition technology in residential buildings is used most against renters with the least amount of power against their landlords. That results in people from already marginalized communities—who in this city are often poor and Black or brown—being over-scrutinized and even evicted for minor rule violations.¹¹

The 2019 Fair Housing Trends Report, put out by the National Fair Housing Alliance, identified technology as a potentially damaging new source of bias in housing because it often “perpetuates the discrimination and bias embedded in U.S. housing markets for centuries.”¹² New York City has an awful history of perpetuating discrimination and bias in housing.¹³ It also has a history of over policing its public housing projects. In the recent past, the Legal Aid Society and its partners have sued both the City and the New York City Housing Authority to protect the civil rights of NYCHA residents and reduce the amount of unconstitutional stops, frisks, and searches of residents and their guests. The Federal Monitor put in place to oversee the NYPD’s policing of NYCHA housing in the *Davis* case is still in place.¹⁴

One Brooklyn tenant whose management company tried to implement a facial recognition system to enter into his building compared it to residents being “tagged like animals.”¹⁵ Biometric surveillance to enter a residential building completely strips those

¹¹ MacMillan, Douglas, “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/>, retrieved June 5, 2024.

¹² 2019 Fair Housing Trends Report [PDF], National Fair Housing Alliance, <https://nationalfairhousing.org/wp-content/uploads/2021/10/2019-Trends-Report.pdf>, at pg. 50.

¹³ “A Brief History of Redlining,” NYC.gov Environment and Health Data Portal, January 6, 2021, <https://a816-dohbsp.nyc.gov/IndicatorPublic/data-stories/redlining/>, retrieved June 6, 2024.

¹⁴ *Davis v. the City of New York and New York City Housing Authority*, 10 CIV 0699 (SDNY), ongoing.

¹⁵ Durkin, Erin, “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>, retrieved June 5, 2024.

residents of their autonomy in their own home. People have a right to associate with others, to invite friends over, to give a pet sitter permission to enter. Facial recognition both controls access to what should be a person's most private space, and strips any autonomy they might feel over their own home. A facial recognition system can never answer the question as to whether a stranger has been invited into an apartment building, and therefore should not be used as a tool to make any determination about residential trespassing. Moreover, people should not be forced to provide their biometric information in order to live in New York City.

Further, this information, once created, can live in a database indefinitely. It can ultimately get turned over to law enforcement, either voluntarily by a request or through a subpoena. That power would not be limited to the NYPD but potentially immigration enforcement or other federal or out-of-state law enforcement. According to a report by the Georgetown Center on Privacy and Technology, Immigration and Customs Enforcement runs a “surveillance dragnet” that taps “vast databases held by private data brokers as well as state and local bureaucracies historically uninvolved with law enforcement.”¹⁶ The only way to avoid massive databases of biometric information from being used to target immigrants and other overly surveilled people is to keep those databases from existing.

As with so much of our personal data, the only true way to keep it safe—and to keep citizens safe from its misuse—is to prevent it from being captured and stored in the first place.

IV. BIOMETRIC SURVEILLANCE HAS NO PLACE IN NEW YORK CITY BUSINESSES

So far, there are very few societal goods that have come out of commercial businesses implementing biometric surveillance technologies. The use of these technologies generates two

¹⁶ “American Dragnet,” Georgetown Center for Privacy and Technology, May 10, 2022, <https://americandragnet.org/>, retrieved June 6, 2024.

kinds of headlines: on the one hand, everyday businesses like pharmacies and grocery stores are using flawed and biased systems to accuse customers of shoplifting. On the other, wealthy individuals are using it to punish their enemies—real or perceived—for social behavior that they as private citizens simply don't like, such as working for a law firm that happens to be suing them.¹⁷

While the latter has been well-publicized local news, the former is the far more pervasive and insidious use of the technology. In December 2023, the Federal Trade Commission sued the pharmacy Rite Aid for its use of facial recognition technology between the years 2012 and 2020.¹⁸ According to the complaint, Rite Aid used facial recognition technology in stores in at least 11 cities, including New York.¹⁹ The FTC alleges that Rite Aid banned people from entering stores or making purchases, subjected them to invasive searches, accused them of past criminal activity, and even called the police based in whole or in part on the “matches” from this technology, many of which were false. The injuries were especially prevalent among those who were Black, Asian, Latinx, and women customers.²⁰ This Orwellian technology was deployed against tens of thousands, possibly even millions of regular people who just happened to enter a Rite Aid during the 2010s, invading the privacy of every single person who entered, for the limited value of possibly helping the company detect some additional amount of minor shoplifting (data on how much it actually helps the companies who use it is scarce).

¹⁷ Katz, Fred, “James Dolan doubles down on use of facial recognition at MSG in latest interview,” *The Athletic*, January 27, 2023, <https://www.nytimes.com/athletic/4132393/2023/01/27/james-dolan-msg-facial-recognition-wfan/>, retrieved June 6, 2024.

¹⁸ Bhuiyan, Johana, “Rite Aid facial recognition misidentified Black, Latino and Asian people as ‘likely’ shoplifters,” *The Guardian*, December 20, 2023, <https://www.theguardian.com/technology/2023/dec/20/rite-aid-shoplifting-facial-recognition-ftc-settlement>, retrieved June 6, 2024.

¹⁹ *FTC v. Rite Aid Corp.*, 2:23-cv-5023 (E.D. Penn.), complaint available at [PDF] https://www.ftc.gov/system/files/ftc_gov/pdf/2023190_riteaid_complaint_filed.pdf, retrieved June 6, 2024.

²⁰ *Id.*

Those wrongful arrests can cause a snowball effect of harm. In one of the latest publicly known cases of a facial recognition false positive leading to arrest, a 61-year-old Texas man alleges he was “beaten and raped by three men in a Texas jail bathroom in 2022 after being booked on charges he’d held up employees at gunpoint inside a Sunglass Hut in a Houston shopping center.”²¹ At the time of the alleged robbery in Texas, he was in jail in California. No one bothered to check before Macys sent the police toward the wrong man based on faulty facial recognition. According to the *Washington Post*, “the confidence authorities placed in the automated results may have ‘primed’ witnesses and investigators to believe Murphy was at fault without substantial evidence.”²² It is irresponsible to allow businesses unfettered use of this technology when examples of this kind of misuse abound.

V. CONCLUSION

Biometric surveillance and facial recognition cause real harm to real people. For individuals, they can lead to false accusations, false arrests, or being prevented from moving freely in public or private due to capricious decisions made by private actors for unknown reasons. More widely, these technologies lead to all of society being surveilled and their movements able to be tracked constantly, with our most private data — information about our own bodies — held indefinitely by private companies under constant threat of theft or hacking. It is no way to live, and the City Council should pass Intros 217 and 425 to protect all New Yorkers from this harmful surveillance technology.

²¹ Harwell, Drew, “Man sues Macy’s, saying false facial recognition match led to jail assault,” *The Washington Post*, January 22, 2024, <https://www.washingtonpost.com/technology/2024/01/22/facial-recognition-wrongful-identification-assault/>, retrieved June 6, 2024.

²² *Id.*

New York City Council Committee on Technology

Testimony by: Fernando Brinn

Monday, June 10, 2024

Good afternoon, Chair Gutierrez and Committee Members. My name is Fernando Brinn and being a native New Yorker, I take pride that I have been and continue to be engaged with the community as well as serving in public office. I am here today to stress the need for the city to continue to strengthen its position on cyber resiliency.

The New York organizations that I am connected to are often left to fend for themselves regarding purchasing the tools needed to protect my data as well as the reputation of the city. Our world faces a time of data leaks and security hacks, and NY is not immune to these bad actors.

Spending time with my community as well as my own organizations continually shows me our vulnerabilities as well as the need for affordable cyber insurance. This made me see that I needed to do my part to help my organizations and maybe even help our government find new ways to ensure that the systems we rely on are protected.

For my organizations, we are focusing on continuing to build our defenses and I'd like to share those connections to help strengthen the protection of the City of New York's systems and help secure the information and systems that we all depend on for our daily lives. I also recommend requiring that future contracts stipulate budget components solely to be used for cyber protection and insurance tools.

My objective is to help the City of New York avoid being the next data breach news headline. Your consideration of these matters and solution is very much appreciated.

I thank Jennifer Gutiérrez, the committee chair and members: Erik D. Bottcher, Robert F. Holden, Vickie Paladino and Julie Won for the opportunity to present this testimony.

**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: Kelly Moran, Chief Information Security Officer

Address: _____

I represent: OTU

Address: _____

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

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

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

in favor in opposition

Date: _____

(PLEASE PRINT)

Name: Charital Seratus, Deputy Commissioner

Address: _____

I represent: OTU

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. 539 Res. No. _____

in favor in opposition

Date: 6/10/24

(PLEASE PRINT)

Name: Albert Fox Cam

Address: 40 Yecol St

I represent: Surveillance Tech Oversight Project

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: FERNANDO BRINN

Address: [REDACTED] BROOKLYN NY

I represent: The BRINN GROUP LLC

Address: 3156 3rd Ave Brooklyn NY

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. 20425 ²¹⁷ Res. No. _____

in favor in opposition

Date: 6/10/24

(PLEASE PRINT)

Name: Shane Ferro

Address: 120-46 Queens Blvd Kew Gardens

I represent: The Legal Aid Society

Address: _____

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. 2178425 Res. No. _____

in favor in opposition

Date: 6/10/2024

(PLEASE PRINT)

Name: NINA LOSHKALIAN

Address: 40 RECTOR ST

I represent: SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

Address: 40 RECTOR ST

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. 425 Res. No. _____

in favor in opposition

Date: 6/10/2024

(PLEASE PRINT)

Name: Adam Roberts

Address: _____

I represent: Community Housing Improvement Program

Address: _____ (CHIP)

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. 217/425 Res. No. _____

in favor in opposition

Date: 6/10/24

(PLEASE PRINT)

Name: JAKE PARKER

Address: _____

I represent: Security Industry Association

Address: 8455 Colesville Road Suite 1200

Silver Spring, MD 21114

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: June 16, 2024

(PLEASE PRINT)

Name: Sharon Brown
Address: 130-18 140 Street
I represent: Rose of Sharon Enterprises
Address: Suite 1 Jamaica Ny 11436

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. 217/425-2024 Res. No. _____
 in favor in opposition

Date: 6/10/24

(PLEASE PRINT)

Name: ROBERT TAPPAN
Address: [REDACTED] BETHESDA MD
I represent: INTL BIOMETRICS + IDENTITY ASSN 20814
Address: 1325 G ST, NW # 500 WASHINGTON, DC
20005

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