NYC OTI
Office of Technology & Innovation

OFFICE OF TECHNOLOGY AND INNOVATION TESTIMONY BEFORE THE NEW YORK CITY COUNCIL COMMITTEES ON TECHNOLOGY & CIVIL AND HUMAN RIGHTS

Oversight - The Use of Biometric Identification Systems in New York City.

MAY 3, 2023

Good afternoon, Chairs Gutiérrez and Williams and members of the City Council Committees on Technology and Civil and Human Rights. My name is Michael Fitzpatrick. I am the Chief Privacy Officer for the City of New York. I am joined today by Ryan Birchmeier, Deputy Commissioner for Public Information at the Office of Technology and Innovation. We thank you for the opportunity to highlight my office's critical work strengthening privacy policy and protecting New Yorkers' identifying information.

For those who are unfamiliar with my role, it was established by Local Laws 245 and 247 of 2017, otherwise known as the Identifying Information Law. Implementation of this law began in 2018. Subsequent legislation formally established the Office of Information Privacy, which I am responsible for leading, and Executive Order 3 of 2022 placed the Office of Information Privacy under the Office of Technology and Innovation as part of the wider consolidation of technology offices. Embedding the Chief Privacy Officer role within the Office of Technology and Innovation has enhanced the consideration of privacy in government operations and initiatives, particularly in matters of technology, by integrating core values such as transparency, data minimization, data integrity, and equity into our agency's work and citywide in close collaboration with our agency partners.

As Chief Privacy Officer, I am responsible for advancing privacy protection in government operations and establishing citywide policies and protocols related to agencies' collection, disclosure, and retention of identifying information. A core objective is the promotion and maintenance of public trust, particularly through clear governance for the handling of identifying information across agencies to provide confidence to New Yorkers that it is safe to seek and access assistance and services.

My office is not alone in citywide privacy protection. Critical partners in this work are the Agency Privacy Officers embedded within each city agency pursuant to the Identifying Information Law. Our Agency Privacy Officers are appointed by their respective agency heads to be stewards of their agency's privacy practices and make decisions about how their agency collects, retains, and discloses identifying information.

Additionally, as the Council is aware, the work of setting citywide privacy policy is supported by the Citywide Privacy Protection Committee. Pursuant to the Identifying Information Law, each agency

must biennially report their policies and practices regarding the collection, retention, and disclosure of identifying information to the Mayor, the Speaker of the City Council, and the Chief Privacy Officer. The Citywide Privacy Protection Committee bears the statutory responsibility of reviewing submitted agency reports and developing recommendations for the Chief Privacy Officer relating to policies and procedures regarding the collection, retention, and disclosure of identifying information.

Through this charge, the committee is a partner in improving the privacy posture of New York City government operations while factoring in the unique missions, subject matter and legal obligations of its agencies. The Identifying Information Law defines the committee's membership, with certain agencies as mandatory members, and lends the Mayor the authority to add other agencies with expertise relevant to protecting identifying information.

Just last month, the Citywide Privacy Protection Committee was relaunched with its role expanded beyond the review of agency privacy reports to include an advisory capacity to the Chief Privacy Officer on matters relating to emerging technology and current events. The reimagined committee provides space for communication across agency expertise to further enhance citywide privacy policies, affords the opportunity for its membership to remain active outside of the biennial review of agency privacy reporting, and facilitates an even stronger community of privacy practice across city government.

I expect the expertise and perspective of the committee will prove invaluable in discussion of privacy policy relating to potential agency use of biometric identification systems. As the council is aware, "biometrics" is a category of information explicitly defined as identifying information in the Identifying Information Law. Any agency collection or disclosure of this kind of identifying information, including through technology specifically used for the purpose of biometric identification, as well as activities where biometric data elements are collected or disclosed without using biometric identification systems, are equally subject to the same privacy safeguards afforded by the Identifying Information Law and associated citywide privacy policies.

While biometric identification systems remain an emerging area of technology and privacy practice globally, the framework provided by the Identifying Information Law, along with the steps taken by this administration, have positioned privacy to be duly considered in potential government utilization of the technology in New York City. We appreciate the opportunity to participate in today's hearing, and, with that, Deputy Commissioner Birchmeier and I will now take Council Members' questions.

###

2023-05-06 – Written Testimony – City Council Hearing on Two Facial Recognition Bills

Fabian Rogers

Constituent Advocate, Office of NYS Senator Jabari Brisport

frogers@nysenate.gov

347-450-8654

Good day, all. Thank you for your time and effort in having this City Council hearing regarding important local-level anti-surveillance legislation. My name is Fabian Rogers, and I'm a constituent advocate from NYS Senator Jabari Brisport's office. Thank you to all of the advocacy groups as well as public officials that made these bills become a reality.

I share my testimony today because I also work in a community advocate capacity since 2018. Due to the rising Brooklyn housing market bubble, a lack of enforcing city/state legislation, gentrification, and flipping the Atlantic Plaza Towers apartment complex I resided in from Mitchell-Lama to rent-stabilized housing, my old landlord thought it would be a trendy idea to attempt to install heat-mapping facial recognition technology in the front entrances of each building.

With the legal and communications help of Brooklyn Legal Services Tenants Rights Coalition, my neighbors and I advocated against our landlord, Robert Nelson, Nelson Management, and the culprit of the erroneous technology, Stonelock. A lack of legislation to allow us to sue our landlord led to us having to do a shame campaign against Nelson Management, HCR (the NYS Department of Homes & Community Renewal), and Stonelock for almost two years.

Similar to this hearing today, our advocacy put us a step in the right direction as Nelson Management revoked its application to HCR for the technology. Amid that victory, the unfortunate reality was that my neighbors and I had nothing in the city/state legislation to stop Nelson Management from applying to install the technology again in the future. Testifying at a hearing like this is an impactful moment for a community advocate like myself because this is a step towards actual regulations and enforcement against private entities attempting to remove the people of this city's access to autonomy and privacy. I've been focusing on privacy and anti-surveillance rights for everyday people who don't have the time, resources, or money to be a part of these impactful discourses regarding the public.

This city council hearing regarding the two bills that would ban facial recognition technology in residential buildings and places of public accommodations is a step in the right direction in bringing

legislative enforcement to technologies being developed and deployed at speeds we've had difficulty maintaining a pace with. This country struggles to have a national standard of regulations and enforcement against these developing AI, facial recognition, machine learning, surveillance, and other biometric technologies. The burden of responsibility, accountability, and enforcement falls on the shoulders of localities among different cities and states to halt the proliferation of these racially/culturally-biased, unvalidated, untested, and error-prone technologies. Because locality legislation has been playing catch-up with the speed of development and deployment of these technologies for years, as a community advocate, this has been a cesspool of dealing with silicon-valley third-party vendors attempting to profit off of privacy and surveillance-mongering.

To allow space for these companies to hastily and carelessly deploy technologies to make profits off of serving corporate conveniences among landlords and private businesses is a failure to protect the people of this city. We do not need failing techno-solutionism to expedite and add nuance to the stigmatization and discrimination of under-represented and marginalized communities. We must continue to challenge how we interact with technology moving forward because it's not the end-all-be-all solution for all the problems to come. We must invest in community-based and community-led solutions instead of these problematic "advanced" technologies. A reliance on technology among private companies and policing authorities only expands on the ongoing biases among these institutions. These potential bans are a step in the direction of how we must do better for the welfare of the people of New York City.

New York State Senator
Kristen Gonzalez
District 59

State Senator Kristen Gonzalez
Testimony to the Internet and Technology Committee

Dear Chair Gutiérrez and Members of the Internet and Technology Committee:

My name is Kristen Gonzalez, and I represent Senate District 59, spanning parts of Brooklyn, Queens, and Manhattan. I chair the Internet and Technology Committee in the State Senate, and I am writing to express my enthusiastic support for Intro 3300 and Intro 3301, both of which provide vital protections against the use of biometric surveillance technology.

Intro 3300 would reduce the intrusion of biometric surveillance into the daily activities of New Yorkers by banning its use in places of public accommodations (including stores and sporting arenas) and requiring written consent before use. The incidents at Madison Square Garden and Radio City Music Hall earlier this year have shown the ways in which biometric surveillance can be used as a tool to intimidate opposition, violate civil liberties, and silence dissent. Such technology does not succeed in keeping us safe and has long been weaponized against low-income communities and people of color. It is clear that in a democracy, and in a city as diverse as New York, we must limit the use of this technology in public places.

Intro 3300 extends these protections to the homes of New Yorkers by preventing landlords from using biometric surveillance technology against tenants and their guests. In multiple large buildings in NYC, tenants have successfully organized to stop landlords' plans to install facial recognition systems, with good reason. With recent reports showing that landlords use biometric surveillance as a means to track movements, build cases for evictions, and harass tenants[1], banning the use of this technology by landlords is essential to protecting the rights of tenants.

New York City has an opportunity to be a national leader on this issue. Limiting the use of this technology would constitute a landmark victory for civil rights and privacy protection for New Yorkers; it would also have ripple effects across the country. I look forward to continuing to work with my colleagues at the city level to protect New Yorkers' civil liberties and mitigate the racialized harm done by this technology.

Sincerely,

Kristen Gonzalez

[1] Keppler, Nick. "Meet The Spy Tech Companies Helping Landlords Evict People." January 4th, 2023. https://www.vice.com/en/article/xgy9k3/meet-the-spy-tech-companies-helping-landlords-evict-people

TESTIMONY OF PUBLIC ADVOCATE JUMAANE D. WILLIAMS TO THE NEW YORK CITY COUNCIL COMMITTEE ON TECHNOLOGY AND COMMITTEE ON CIVIL AND HUMAN RIGHTS MAY 3RD, 2023

Good afternoon,

My name is Jumaane D. Williams, and I am the Public Advocate for the City of New York. I would like to thank Chair Williams, Chair Gutiérrez, and the Committee members for holding this hearing. Privacy rights are rapidly eroding due to the proliferation in new technologies. While many have accepted decreasing privacy rights as an inherent tradeoff with receiving amazing services, technology can never override our constitutional rights. Lawmakers must continue to protect the right to privacy, in both public and private settings. I support bills Int 1014-2023 and Int 1024-2023 because we must hold individuals and businesses accountable for violating our privacy rights.

Regulation is key to solving the potential privacy violations of biometric data collection. Since the State of Illinois has passed the Biometric Information Privacy Act in 2008, "approximately 2,000 lawsuits that allege BIPA violations have been filed, yielding a series of massive settlements and judgments"[1]. The law has been used to sue businesses for collecting biometric data without consent, such as in a case where an employer made every employee sign into work with their fingerprint. The New York City Council bill 1014-2023 proposed today by Council Member Rivera will allow a prevailing party to recover up to five thousand dollars per violation for collecting biometric data which will help serve as a deterrent for some individuals to not do so.

There must be a strong deterrent to utilizing biometric technologies, because the technology has proven to be inaccurate towards darker skinned individuals. In 2019, MIT reported facial recognition software marketed by Amazon misidentified darker-skinned women 31% of the time[2], while others have "shown that algorithms used in facial recognition return false matches at a higher rate for African Americans than white people unless explicitly recalibrated for a black population.[3]" Furthermore, the largest facial recognition company that partners with nearly 2,000 public agencies nationwide, Clearview AI, has no publicly available information that proves that

[1]https://www.edgeir.com/illinois-supreme-court-rules-white-castle-may-face-billions-in-penalties-for-biometric-data-collection-20230224
[2]https://www.vox.com/the-goods/2019/1/28/18201204/amazon-facial-recognition-dark-skinned-women-mit-study
[3] https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html

its facial recognition software is accurate and has not been vetted by a third party[4]. These error-prone, racially biased algorithms have devastating impacts for people of more color. One false match can lead to a wrongful arrest[5], a lengthy detention, or even deadly police violence. 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. Int 1024-2023 would limit the ability of landlords to potentially use biometric data against their tenants. The bill gives tenants the right to acquiesce to the use of a minimal amount of authentication and reference data, but cannot use biometric identifier information. Additionally, a tenant's consent to use of that data must be documented through a written document or video.

Technology can be a powerful tool to provide equity, transparency, and progress, but it can also be abused. Recently, in NYC, we saw executives from Madison Square Garden using this technology to deny entrance to valid ticket holders who worked for law firms who were involved in litigation against them. Furthermore, technology is all too often used to further systemic inequities within vulnerable communities. Facial recognition technology 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.

[4] https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition
[5] https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

Testimony: The Use of Biometric Identification Systems

4.27.23

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 provide strategic uses in many aspects of daily life and business. As technologies that focus on security or crowd safety features continue to develop, facial and biometric recognition technologies have the potential to help businesses in new ways -- many of which are still unforeseen. NYC's existing law requires public notification when this technology is used, and it is important for any businesses using it to do so with complete transparency and respect for personal privacy. 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 access to culturally sensitive technologies as they continue to develop and evolve. Additionally, while the widespread and unchecked roll-out of new facial and biometric recognition technologies may result in unforeseen circumstances, Tech:NYC also recommends for any new legal or regulatory limitations to be developed with responsible use cases in mind.

Facial 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 recognition can aid businesses implementing new customer service and security measures, as well as those which have been targeted for crimes. Providers of childcare or services for sensitive populations can use these technologies to help confirm visitors, and businesses can also use them 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. Regardless of the type of business or venue using these technologies, it is 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 it for accessing venues, businesses, or services.

Regarding Int. 1014, 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, as it 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. 1024 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 “prop tech” 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 and housing developments 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 any NYC business using biometric identifying technologies to disclose its use via clear signage. There is much potential for this technology, and at the same time there is also potential for its abuse. Any abuse of this technology only detracts from the

positive advancements that it can make to assist businesses and private citizens alike. Given the growing number of use cases and the positive trends in AI workforce, there is a significant local benefit for encouraging the development of 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.

REBNY Testimony | May 3, 2023

The Real Estate Board of New York to

The New York City Council Committees on Civil and Human Rights and Technology Regarding Facial Recognition and Biometric Technology

The Real Estate Board of New York (REBNY) is the City's leading real estate trade association representing commercial, residential, and institutional property owners, builders, managers, investors, brokers, salespeople, and other organizations and individuals active in New York City real estate. Thank you, Chair Williams and Chair Gutierrez, and committee members for the chance to discuss facial recognition identification systems and other biometric technology as part of today's hearing.

In recent years, REBNY has appreciated the opportunity to work with the City Council as biometric technology, including facial recognition, has continued to evolve, and become more prevalent in society and across industries. The real estate industry is no exception.

In many ways, these emerging technologies have benefitted the real estate industry. Examples include the utilization of biometrics to allow easier building access for both residential and commercial tenants while maintaining appropriate security, faster retail experiences that allow for traditional checkout kiosks to be bypassed, and data retention systems that analyze use trends to create more comfortable and energy efficient buildings.

Through all these examples and beyond, REBNY members have established best practices to ensure that this technology can be embraced while protecting the personal information of those who interact with our built environment every day. This includes ensuring that data is retained and disposed of appropriately, and that transparency remains a key principle as innovative technologies emerge. It is through these lenses that REBNY looks forward to working with the Council on the legislation being heard today.

While changes should be made to the legislation being heard today to provide additional clarity and to avoid unintended consequences, REBNY agrees with the intent of both bills and looks forward to working with the Council to strengthen this legislation if there is an opportunity to do so.

BILL: Intro 1014-2023

SUMMARY: This bill 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. Also, the bill would require any such information collected to be protected and for written policies regarding its use to be made available.

SPONSORS: Councilmembers Hanif, Gutierrez, Rivera, Williams, Sanchez, Louis, Marte and Farias.

REBNY believes that additional clarity is required for this legislation. REBNY agrees that for any biometric recognition technology to be utilized, consent should be required regarding those whose information could be collected or retained. In addition, appropriate transparency and data retention policies should be required and followed.

As written, Intro 1014 is incredibly broad in scope, and would benefit by more explicitly defining what constitutes a public space. Broadly, a public space is any location with unfettered access by persons known and unknown to the provider. It would behoove the Council to differentiate this type of space from space not typically accessible to the public. Practically, this would allow for such technology to be harnessed to support access to spaces utilized for company employees, with consent, to continue to be utilized.

In addition, REBNY hopes that technology utilized for standard security purposes, such as a security camera, is not included. Precedence for this type of clarity can be found in a similar statute enacted in recent years in Washington D.C.

Lastly, while the bill states that it is unlawful to use biometric recognition technology, it also requires notification, written consent, protection of stored information and written policies for an unlawful act if biometric recognition technology is utilized. This is in direct contradiction, and clarity is needed. REBNY and its members are happy to assist in suggesting appropriate changes to provide this needed clarity.

BILL: Intro 1024-2023

SUMMARY: This bill would make it unlawful for an owner of a multiple dwelling to install, activate or use any biometric recognition technology that identifies tenants or the guest of a tenant.

SPONSORS: Councilmembers Rivera, Sanchez, Caban, Hanif, Louis, Riley, and Richardson Jordan by the request of Manhattan Borough President Levine.

REBNY believes that Intro 1024 completely prohibiting the use of facial recognition is an over-correction. Instead, the Council should consider an appropriate regulatory framework for technology that can provide significant benefits to a building and its tenants. The use of facial recognition as a means of access control is an emerging technology in both residential and commercial properties. In most instances, it is optional and offered for the convenience of tenants. In all instances, however, REBNY supports the use of best practices relative to transparency and the need for consent, and for data to be retained and disposed of in an appropriate way.

In lieu of banning facial recognition technology in residential settings, REBNY recommends that the Council revisit Local Law 63 of 2021, which requires owners of multiple dwellings that utilize technology like keyless entry systems, to provide tenants with a data retention and privacy policy. The law also established restrictions on the collection and use of data collected, which could be updated to ensure concerns about facial recognition technology are considered. As REBNY worked diligently with then-Councilmember Mark Levine on the legislation that became Local Law 63, we would look forward to continuing this conversation to consider the latest technologies.

Thank you for your consideration of these points.

CONTACT:

Ryan Monell

Vice President of Government Affairs
Real Estate Board of New York
212-616-5247
rmonell@rebny.com

Annenberg School for Communication
University of Pennsylvania
3620 Walnut Street
Philadelphia, PA 19104-6220
215-898-5842
jturow@asc.upenn.edu

Joseph Turow
Robert Lewis Shayon Professor of Communication

May 1, 2023

Greetings, City Council-

As a professor who has studied issues of digital surveillance and privacy for three decades—and who grew up in New York and has an apartment in the city—I was pleased when asked to testify on Int. No. 1014 and Int. 1024. The concern about biometric identification and recognition that drives both proposed laws is one that I share. One of my recent books—*The Voice Catchers*, published in 2021 by Yale University Press—centers on the dangers for freedom and democracy posed by the commercial use of emerging biometric technologies such as voice identification, recognition, and inferences in both the commercial and political spheres. I am sending along a copy of the book's final chapter for your possible interest.

I find that both proposed laws are necessary in today's world. They correctly recognize that landlords and businesses are increasingly using biometric technologies such as facial recognition and retinal scans, and they attempt to put guardrails around the use of such technologies. I do have three suggestions for additions to Int. No. 1014 that are crucial for ensuring that New Yorkers and visitors who use places or providers of public accommodation will be safe from biometric exploitation:

1. The proposed law states in paragraph 22-1202a that a provider of public accommodation that collects biometric identifier information of customers must disclose "such collection, retention, conversion, storage, sharing, or obtaining of biometric identifier information, as applicable, by placing a clear and conspicuous sign near the place or provider of public accommodation's customer entrances notifying customers in plain simple language…" The proposed law goes on to require "written consent of such customer in advance of any collection." **I suggest it is important to require the establishment to notify customers via the sign exactly why the collection of biometric identifier information is taking place as well as who and in what organizations will get to see it.** Doing that will make the activity truly informed consent.

2. The focus of paragraph 22-1202 and the rest of the proposed law is on consent for identification and recognition. But the proposed law ignores the real possibility that companies will use the consent for identification and recognition to gather additional biometric data and associate other data about the individual to the biometric data. So, for example, scientists believe that a person's voice can reveal many things about the

person, including height, weight, ethnicity, some diseases—even whether a woman is on birth control medicine. An establishment may in the future infer such data from a person's voice print and link the data to other personal information (maybe the home address, age, race, education) plus to the person's activities in the establishment. Then the establishment may use artificial intelligence to draw conclusions about the customer's lifestyle, interests, and capabilities that affect the ways the establishment deals with that person. Not only would the customer not know about these conclusions, but the person might also not agree with them if the person knew. Such activities open the door for prejudicial discrimination often called algorithmic bias. **With these considerations in mind, I suggest that the proposed law prohibit linking the biometric identifier information to any data about the person beyond the specific relationship to the public establishment—for example, room number, table number, or purchase interest.**

3. Finally, Int. par 22-1202 allows companies to claim their "initial purpose for collecting or obtaining such identifiers or information has been satisfied" within two years of the interaction. A restaurant, for example, can claim that it is keeping the biometric data for that length of time just in case the person shows up again. But allowing firms to store such data for long periods of time increases the possibility that the data may be stolen and used in inappropriate ways. Biometric data in the hands of thieves or on the dark web is particularly problematic because unlike passwords and e-mail addresses a person's fingerprint, voice print and retinal information cannot be altered without great effort. **I would therefore suggest that the proposed law requires that the biometric data be destroyed when the person leaves the establishment--that is, pays the restaurant bill, leaves the theater, checks out of the hotel.**

I much appreciate the opportunity to present my ideas to the City Council. I hope you find them useful.

Sincerely,

Joseph Turow, Ph.D.

Brooklyn Defenders

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

Tel (718) 254-0700
Fax (718) 254-0897
info@bds.org

TESTIMONY OF

Elizabeth Daniel Vasquez,
Director, Science and Surveillance Project

BROOKLYN DEFENDER SERVICES

Presented before

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

Oversight Hearing on the Use of Biometric Identification Systems in New York City

May 3, 2023

My name is Elizabeth Daniel Vasquez. I am the Director of the Science & Surveillance Project at Brooklyn Defender Services (BDS). BDS is a public defense office whose mission is to provide outstanding representation and advocacy free of cost to people facing loss of freedom, family separation and other serious legal harms by the government. I thank Chairs Gutiérrez and Williams for inviting us to testify today about the use of biometric identification systems in our city.

For over 25 years, BDS has worked, in and out of court, to protect and uphold the rights of individuals and to change laws and systems that perpetuate injustice and inequality. We represent approximately 22,000 people each year who are accused of a crime, facing loss of liberty, their home, their children, or deportation. Our staff consists of specialized attorneys, social workers, investigators, paralegals and administrative staff who are experts in their individual fields. BDS also provides a wide range of additional services for our clients, including civil legal advocacy, assistance with educational needs of our clients or their children, housing and benefits advocacy, as well as immigration advice and representation.

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

I want to thank the Committees on Technology and Civil & Human Rights for holding this important discussion not only on biometric identification systems, but also on their impact on our communities, their relationship to the expanding world of artificial intelligence, and the overwhelming governmental resistance to regulation in this space.

Biometric identification systems are fundamentally a species or outgrowth of artificial intelligence.

This hearing is particularly timely. As public defenders for the borough of Brooklyn, we see these systems in daily use, impacting our clients in the criminal legal systems, the family separation systems, and the immigration systems. We've even seen them deployed against our clients seeking unemployment benefits, facing evictions, or calling their loved ones from detention.

Underlying the mad spread of biometric identification systems is the national and global expansion of artificial intelligence generally. Computerized pattern matching engines are dominating the news and their dangers are being debated globally.

The bills proposed here—Int. 1014 and Int. 1024—address one symptom of this proliferation but they do not ultimately address the underlying disease. To get to the core of this era-defining issue, it is critical to understand how machine learning or artificial intelligence (AI) works.

Fundamentally, to build an AI system, a developer needs a large amount of data. Features of surveillance data—like the faces in surveillance footage—form datasets used by big tech. Those large datasets "teach" AI systems. Without those datasets, biometric identification systems would be impossible. AI, then, brings with it a voracious appetite for data.

Thus, the conversation our community truly needs to have is not one centered around banning individual technologies but instead around defining our rights to our data. And particularly, grappling with the inequities of the data surveillance economy we are already constructing around ourselves.

The single biggest user of biometric identification technology in our city is government.

Agencies as diverse as the NYPD, Department of Correction, the Administration for Children's Services, NYCHA, the Department of Labor, Department of Homeland Security, Immigration and Customs Enforcement and Customs and Border Protection, use biometric identification systems. And the neighborhoods carrying a disproportionate amount of our city's surveillance load are Black and Brown. Strikingly, the bills before the committees today do not directly address these facts.

Our city has invested billions in a twenty-year surveillance infrastructure building program that relies critically on biometric identification technologies. Despite these investments and deployments, the promise of enhanced public safety has not been realized. Instead, all this surveillance infrastructure has accomplished is to expand the burgeoning surveillance state, repeatedly infringe on New Yorkers' dignity, privacy, and First Amendment freedoms, and

further entrench the systemic racism inherent in our criminal legal, family separation, and immigration systems. This reality has nothing to do with accuracy or the need for improvement. There is no way to construct a surveillance state in a way that honors our fundamental rights and dignity or builds real justice.

Some examples that exemplify this point:

A. Voiceprints: Securus Technologies

In 2018 and 2019, our Council led the country in making phone calls from city jails free of charge. By 2021, however, it became very clear even though calls no longer cost our clients and their families money, these calls carry a far more significant cost.

The first indication of this came when it was revealed that DOC and its phone service and surveillance vendor Securus had illegally recorded more than 1,500 privileged phone calls between people incarcerated and their attorneys. This illegal activity was not new for Securus. Since 2018, they've been sued nationwide for this practice. But illegal call recording turns out to be the tip of the iceberg when it comes to Securus' troubling surveillance scheme.

The company has built a vast and interconnected web of surveillance that is perpetually blanketing not only those presently detained in our city's jails, but also their families, communities, and advocates. For example, Securus houses a database of the audio recordings of every call made from our city's jails, the transcribed text of those calls, the personal information of everyone who has been processed into those jails, and the financial information of every community member who has put money on a commissary account.

That broader database operates on the indexing power of Securus's voiceprint collection and storage. A biometric identifier, voiceprints record the arguably unique signature of a person's speech patterns. To make its NextGen Platform work, Securus collects the voiceprints of everyone who has ever placed or received a call from New York city's jails. The company and DOC do not delete these voiceprints after a person leaves custody—even if they are found not guilty or have charges dismissed.

Presently, Securus's surveillance web, however, is constructed without any court oversight and no need for a warrant. By contrast, if a person was able to afford bail and so was not being held in city jails, law enforcement would only be able to eavesdrop on that person's calls with a specifically-issued warrant. Borrowed or gifted money would not be tracked. And voiceprints would remain a person's private information. Under Securus's system, the mere reality of being poor and unable to afford bail means a detained New Yorker today, along with his or her entire community, has fewer rights, less privacy, and diminished dignity.

It bears repeating, in case the implications of this web are not clear, that more than 80% of those detained are being held pretrial. Convicted of nothing and predominantly held due to an inability to afford bail, those held pretrial are also more than 90% Black and Brown. This web of surveillance is impacting communities of color at a staggering rate.

B. DNA: OCME/NYPD's rogue DNA database

In 1997, the New York City Office of Chief Medical Examiner (OCME) implemented a system for collecting previously-typed DNA profiles into a searchable local database. Meanwhile, at the state level, the New York State Legislature had created the State DNA Databank in 1994 with the passage of Executive Law § 995. That database became operational in 1996. By law with the passage of § 995, when it comes to known samples, New York databases can only house DNA collected from people *convicted* of a crime. While the list of crimes for which a conviction permits DNA sample collection has grown five times since 1996, the New York State Legislature has repeatedly rebuffed efforts to expand DNA collection to people who are arrested but never convicted of a crime.[1]

Despite New York State's careful balance between the individual's rights to genetic and basic privacy, as well as due process, and the State's interest in crime solving, the City of New York's agencies—the NYPD and the OCME—have chosen to operate a rogue DNA database that reaches samples taken from persons not legally authorized for collection. In other words, the OCME's "LDIS" does an end run around New York State's carefully prescribed scheme. Over the last five years, the OCME's rogue database has been growing.

This unauthorized database has been fed in part by the secret collection of individuals' saliva samples by the NYPD. We have watched videos where our clients have asserted their right to counsel as they drink from a water bottle or smoke a cigarette offered to them by the police. NYPD has even been observed offering teenagers cigarettes in addition to juice bottles or water bottles for DNA collection. No person, let alone a child, would envision that accepting a cigarette to smoke in the middle of a public building with the blessing of the police would mean that their DNA profile would end up in perpetuity in a database. But once our clients are led out of that interrogation room, the cigarette butts and juice bottles are left in an intentionally placed ashtray or garbage bin. The police then collect the cigarette butts and bottles for DNA. This same little game plays out with water cups and juice or water bottles, and DNA profiles are collected by the thousands.

Though the local database was also set up long before the NYPD's Domain Awareness System[2] was created, its contents have since been connected to the Domain Awareness System (DAS). While the DAS's role in aggregating surveillance camera video is well known, another DAS function is its ability to inform officers whether or not an individual detainee's DNA profile is in the database – thus making the detainee a target for DNA collection by individual police officers.

---

[1] It is worth noting that, in 1999, the legislative record reflects that then-Mayor Rudy Giuliani even specifically requested that the legislature expand collection to arrestees. Mayor Giuliani asserted: "While the City enthusiastically supports this legislation and acknowledges the positive effect it will have on solving crime, it should be noted that the City of New York believes DNA testing upon arrest would allow for even greater efficiency and effectiveness in law enforcement. Examining DNA samples at the time of arrest would dramatically increase the ability of police to accurately identify or negate one's potential culpability while under arrest." The New York State Legislature refused to expand the database to arrestees.

[2] The Domain Awareness System (DAS) is a software program created by the NYPD and Microsoft that aggregates data collected by the NYPD across the city.

The current practices of the NYPD and OCME mean that it is not only the countless numerical profiles of mainly people of color that are warehoused in an electronic database. For each of those warehoused profiles, the OCME maintains extracts of the DNA in tiny vials. As technologies emerge, law enforcement and the lab can go back to that vial and effectively interrogate the DNA to invade the genetic privacy of the individual's genetic code in even deeper and more disturbing ways.

Genetic genealogy, which has been much reported-on in the news recently, is only the latest incarnation. This technique uses DNA analysis methods that mine more of the human genome for sensitive information than a traditional forensic DNA test and surveil not just the individuals' DNA but also the DNA of that individual's entire family line.

In the face of this brave new world of genetic testing and the overall threat to privacy, as well as our First Amendment associational freedoms, we need to think about historically targeted communities when considering emerging technologies. The OCME and the NYPD, without oversight or regulation are effectively building a warehoused library of entire communities' genetic extracts. With emerging technologies like genetic genealogy and so-called Next Generation Sequencing, the genetic privacy of not only the individual but the individual's family will come under surveillance by law enforcement.

C. Faceprints: Clearview AI and the HIDTA backdoor

The NYPD has repeatedly publicly suggested that only the Facial Identification Section of the NYPD conducts facial recognition analysis, that this process is thoroughly documented, and that the analysis is governed by clear rules and protocols. Our experience in cases reveals these public assurances to be false.

The NYPD, in fact, uses two additional avenues to apply facial recognition: officer promotional accounts with Clearview AI and a software backdoor in DataWorksPlus.

In April 2021, Buzzfeed broke the news that despite NYPD's public claims that the Department had never formally contracted with the controversial facial recognition company Clearview AI, documents obtained by the news outlet indicated that the NYPD's public statements had been misleading at best. Those records revealed that the NYPD had included Clearview AI amongst its list of acknowledged vendors, beginning in 2018, and that NYPD officers had independently set up and used promotional accounts from the company to conduct unmonitored, undocumented, and unregulated facial recognition analysis in their cases. When those promotional accounts are used by officers in cases, no reports are written, the results are undocumented, and the technology's use is often glossed-over or denied.

But Clearview AI promotional accounts are not the only undocumented avenue for facial recognition use, officers can also use access to PhotoManager (a system used to create photo arrays) to deploy the facial recognition algorithms owned by the High Intensity Drug Trafficking Area (HIDTA) and shared with the NYPD. As with Clearview AI promotional accounts, when

officers use this backdoor in cases, no reports are written, the results are undocumented, and the technology's use is often glossed-over or denied.

These examples drive home two critical insights: (1) the "surveillance load" in our city is being disproportionately carried by Black and Brown neighborhoods and communities; and (2) despite the common belief that the courts provide oversight of government tactics, the collection, storage, and use of the vast majority of surveillance data–including biometric data–will never be reviewed by any court or anyone outside law enforcement.

(1) Surveillance load. "Data-driven," "smart" and "intelligence-led" policing methods were created in response to the biased policing of the Broken Windows and stop-and-frisk eras. But they replicate the same racist biases of those periods and fit neatly into the current "New Jim Code" era, in which "new technologies . . . reflect and reproduce existing inequities."[3]

- More than 90% of those whose voiceprints are being taken by Securus Technologies are Black and Brown;

- The OCME/NYPD have refused to disclose the racial composition of the rogue DNA database, but available data suggests the data comes overwhelmingly from communities of color; and

- When it comes to the placement of facial-recognition compatible CCTV cameras, Amnesty International found that "[i]n the Bronx, Brooklyn, and Queens, . . . analysis showed that the higher the proportion of non-white residents, the higher the concentration of [those cameras]." [4]

Scholars have drawn a line from slavery through convict-leasing programs and on to mass criminalization. That line was not miraculously broken by the introduction of AI.

(2) *Court regulation.* As it relates to the courts' ability to oversee the NYPD's use of biometric data, a close examination of the NYPD's POST Act disclosures brings home the devastating reality that court's are not and cannot be the solution. Despite the common belief that the courts provide oversight over police tactics, the collection, storage, and use of the vast majority of the NYPD's surveillance data will never be reviewed by any court or anyone outside law enforcement. According to its own disclosures, the NYPD does not believe it needs to seek a warrant or court approval to use three-quarters of the surveillance collection methods it has disclosed using.

Conclusion

We thank the Council for holding this hearing and giving us an opportunity to highlight these issues in surveillance. In the face of our city's permeating surveillance ecosystem, there is significant urgency for the Council to truly and thoroughly reckon with the use of biometric identification systems. We welcome an opportunity to speak with each of you more about the

[3] Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code*. Oxford, England: Polity (2019).
[4] Amnesty International, *Inside NYC's Surveillance Machine* (2022), https://banthescan.amnesty.org/decode/

breadth of the problem we are seeing in Brooklyn and the comprehensive solutions we have begun to identify from our unique vantage point in the city.

The bills before the Committees today are a step and they would positively impact the communities of Brooklyn that BDS serves, but they are not enough.

If you have any questions or concerns, do not hesitate to contact me at evasquez@bds.org.

Paul Zuber
Executive Vice President

May 4, 2023

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. 1014, 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:

- Secure building and door access control systems for workers
- Authenticated app-based accounts and payment systems, both online and in-person
- A more convenient form of payment and access at sporting and other entertainment venues
- Fingerprint time-clocks and cash register locks by business employees
- Driver authentication for ride-share services
- Security systems protecting persons or property, including systems augmenting loss prevention efforts
- 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,

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

May 3, 2023

Community Housing Improvement Program Testimony on Int 1024-2023

Thank you for holding this hearing today. I am Adam Roberts, Policy Director for the Community Housing Improvement Program, also known as CHIP. We represent New York's apartment building workers and owners and we are here to express concerns about Int 1024-2023.

Biometric recognition technology is still very new, particularly in its application to residential buildings. While it may not be widely used now, it is likely to become more common across New York's residential buildings in the next few years. Banning it outright now would stop New Yorkers who want to use biometrics in the future from utilizing its benefits.

Biometrics may prove particularly useful in maintaining a building's security. In most of our city, apartment buildings cannot afford to have a full-time doorman or security guard. Biometrics can limit access to tenants, guests, and building workers at a fraction of the cost of a full-time doorman. This would provide significantly greater security for tenants and building workers.

Furthermore, biometrics can make a building's security more convenient for tenants. Though not yet widespread, biometric technology already exists to allow tenants to enter their apartments without a key. Fingerprints or irises could serve as an additional option for entering an apartment or building in the future. In buildings without doormen, this would reduce the burden of forgetting or losing a key.

This convenience biometrics provide is already evident. It is this convenience factor which has made biometrics widely used for entering sporting events, concerts, and airports. Considering this, there should be no reason to ban tenants from using biometrics when entering their own homes or workers from entering their workplace.

Biometrics have the ability to be a great equalizer for New York's tenants by providing additional security at a fraction of the cost of traditional methods. They can have very consequential impacts, like ensuring access only for tenants, guests, and building workers. Banning biometrics would fall hardest on those tenants who cannot afford to live in a doorman building or those workers who are not employed by luxury building owners.

We recognize concerns about privacy and profiling with biometrics. Therefore, we hope the council will redraft this bill or consider new legislation to more thoughtfully address those concerns without outright banning biometrics. Thank you.

Adam Roberts, Director of Policy
Community Housing Improvement Program (CHIP)
516-510-2773
aroberts@chipnyc.org

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

May 5, 2023

New York City Council
Committee on Technology
Committee on Civil and Human Rights
New York City Hall
City Hall Park
New York, NY 10007

Re: Testimony of EPIC on Bills 1014-2023 and 1024-2023

Dear Chair Gutiérrez, Chair Williams, and Council Members,

EPIC writes to urge you to pass both Bill 1014 and Bill 1024 into law to protect New Yorkers from rapidly growing facial surveillance systems that destroy our privacy and harm society. We also urge you to add a private right of action to Bill 1024, and to ensure that both bills protect employees, delivery drivers and other people who may not be covered by the language of the current bills.

The Electronic Privacy Information Center (EPIC) is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] EPIC has long advocated for a ban on facial recognition and strict limits on the collection and use of biometric data.[2]

EPIC studies advanced surveillance technologies including facial recognition, the flaws in these systems, and their impacts on society. As advocates for privacy and civil liberties, we are impressed with the City Council's proposed approach. Earlier this year, EPIC Senior Counsel Jeramie Scott urged the Council to pass a ban on facial recognition in places of public accommodation.[3]

Facial recognition is a dystopian technology, frequently flawed, and even more dangerous when it works perfectly.[4] The Council's approach here is largely correct: a ban on use in places of public accommodation and apartment buildings is the only appropriate response to a technology that can destroy our privacy and effectively close off traditionally public spaces.

We urge the council to consider completely banning private use of facial recognition technology by businesses and landlords. These bills come very close but leave a few exceptions for

[1] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[2] EPIC, *Ban Face Surveillance*, https://epic.org/campaigns/ban-face-surveillance/; *see e.g.* Brief for EPIC as Amici Curiae, Patel v. Facebook., 932 F.3d 1264 (9th Cir. 2019), https://epic.org/amicus/bipa/patel-v-facebook/
[3] EPIC, *EPIC to NYC Council: Take Action on Facial Recognition Now* (Feb. 24, 2023), https://epic.org/%EF%BF%BCepic-to-nyc-council-take-action-on-facial-recognition-now/
[4] *See* EPIC, *Face Surveillance and Biometrics*, https://epic.org/issues/surveillance-oversight/face-surveillance/.

using facial recognition to identify potential shoplifters and others who don't qualify as consumers in Bill 1014 or tenants and guests in Bill 1024.

The protections for "consumers" in Bill 1014 may not ban the non-consensual use of facial recognition systems on employees, delivery drivers, emergency first responders, and other people who might enter a store without the intent to shop there. The safest way to avoid anyone being wrongfully surveilled by a facial recognition system is to ban the system itself.

Similarly, Bill 1024 leaves the door open to install systems monitoring service entrances or tailored to delivery drivers, contract workers, or other non-tenant visitors. Workers deserve equal privacy protections. And bill 1024 lacks a private right of action, which is necessary for the bill to work as intended.

Private use of facial recognition, like the system deployed at Madison Square Garden, is not an effective method for providing security. Rather, it is a form of gatekeeping, an attempt to close businesses and housing to whoever the owner feels in undesirable. At its worst, private use of facial recognition can enable discrimination by allowing comprehensive monitoring of businesses traditionally open to the public, with owner-curated hotlists of people to exclude. Such a practice has no place in a tolerant, democratic society.

Facial recognition systems like the one deployed at MSG will also create more comprehensive and nuanced records of our public movements. A system that identifies individuals when they enter a store effectively records their location and time of arrival. Those records may be accessible by police without a warrant and can also be sold to advertisers, data brokers, and anyone willing to pay for them. Although current city code prohibits such sales, the city made clear to the Council at this hearing that it is not tracking private use of facial recognition and cannot be relied upon to prevent all sale and abuse of biometric data.

And in contrast to most other forms of identification, and even most other forms of location tracking, biometric monitoring is effectively unavoidable. If a person wants more privacy, she can leave her phone at home, but she can't leave her face behind. The same is true for her voice, the way she walks, and other potential ways to identify her based on her physical characteristics.

Banning biometric surveillance in places of public accommodation and apartments will not hurt businesses; if anything, it will save them from spending money on advanced surveillance systems with no evidence-based record of reducing crime or preventing harm. At most, these systems can work to concentrate crime in the poorest and least-resourced neighborhoods, but there is no evidence that surveillance technologies including facial recognition reduce crime as a whole.

We also want to commend the council on the strong private right of action in bill 1014. Especially in a city as large as New York, a private right of action is one of the strongest ways to ensure citizens' rights are protected. While you may hear concerns about a flood of litigation, the reality is that this bill is exceedingly easy to comply with and provides a very reasonable opportunity to cure violations. Lawsuits are likely to only target bad actors.

Finally, at the hearing the Council was rightly concerned with the NYPD's use and misuse of facial recognition technology. The NYPD has a deeply flawed track record of abusing facial

recognition technology and openly flaunting the very transparency laws intended to address such abuses.[5] EPIC and a coalition recently urged the Council to schedule a hearing specifically addressing the NYPD's repeat failures to comply with the Public Oversight of Surveillance Technologies (POST) Act.[6] We also urge the Council to review two reports from the Georgetown Center on Privacy and Technology that lay out in detail the ways that the NYPD ignores science and plays fast and loose with its facial recognition systems.[7] These abuses do not just impact New Yorkers. EPIC recently filed an amicus brief in New Jersey, where a man was identified by NYPD at the request of New Jersey police with no connection to New York whatsoever.[8] His public defenders received no discovery on the reliability of Mr. Arteaga's quite possibly erroneous identification, making an effective defense for a potentially innocent man difficult.

We urge the council to protect citizens' privacy and guarantee equal access to important spaces by passing these bills. If possible, we urge the council to amend them to include a complete ban on private use of facial recognition and other biometric monitoring technologies in these locations.

Thank you for the opportunity to testify, please reach out with any questions to EPIC Senior Counsel Jeramie Scott at jscott@epic.org or EPIC Counsel Jake Wiener at wiener@epic.org.

Sincerely,

Jake Wiener
Jake Wiener
EPIC Counsel

Jeramie Scott
Jeramie Scott
EPIC Senior Counsel,
Director, Project on Surveillance Oversight

[5] *See e.g.*, EPIC Comments to the NYPD on POST Act Disclosures (Feb. 25, 2021), https://epic.org/documents/nypd-post-act-disclosures/.
[6] Coalition Letter to City Council Calling for Hearing on NYPD Post Act Violations (Apr. 13, 2023), https://epic.org/wp-content/uploads/2023/04/Coalition-Letter-NYPD-POST-Act-Violations-Apr2023.pdf.
[7] Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Georgetown Center on Privacy and Technology (Dec. 6, 2022), https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/; Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Georgetown Center on Privacy and Technology (May 16, 2019), https://www.flawedfacedata.com.
[8] New Jersey v. Arteaga Docket No. A-3078-21T1, Brief EPIC, EFF, and NACDL as amici curiae, https://epic.org/documents/new-jersey-v-arteaga/.

FOOD INDUSTRY ALLIANCE OF NEW YORK STATE, INC.
130 Washington Avenue • Albany, NY 12210 • Tel (518) 434-1900 • Fax (518) 434-9962
Government Relations (518) 434-8144

Testimony by
the Food Industry Alliance of New York State, Inc.
in Opposition to Int. 1014-2023

Thank you for the opportunity to testify regarding Int. 1014-2023. My name is Jay Peltz and I am the General Counsel and Senior Vice President of Government Relations for the Food Industry Alliance of New York State (FIA). FIA is a nonprofit trade association that advocates on behalf of grocery, drug and convenience stores throughout the state. We represent a broad spectrum of the New York City retail food sector, from independent neighborhood grocers to large chains, including many unionized stores.

This legislation 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 will be required to get the written consent of each customer in advance of 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 show 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 is by far the largest number of such complaints 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.

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 well-being and safety of customers and workers. We look forward to participating in such a cooperative process with Councilmember Hanif and other government stakeholders. I'd be happy to answer any questions you may have.

Respectfully submitted,

Food Industry Alliance of New York State, Inc.
Jay M. Peltz
General Counsel and Senior Vice President of Government Relations
Metro Office: 914-715-1750
jay@fiany.com

May 3, 2023

International Biometrics+Identity Association

Testimony of Robert Tappan
Managing Director, International Biometrics + Identity Association
before the New York City Council
May 3, 2023

Good afternoon, City Council Members and Chairs Gutiérrez and Williams, and thank you for giving me the opportunity to address you today. My name is Robert Tappan, and I am the Managing Director of the International Biometrics + Identity Association, based in Washington, DC. We are a non-profit industry association chartered to advance the adoption and responsible use of technologies for managing human identity to enhance security, privacy, productivity, and convenience for individuals, organizations, and governments. We do this through advocacy, engagement, and education.

Our reason for appearing before you here today is to communicate our concerns to the Council about the potential for overreach and unintended consequences in the proposed draft legislation contained in Files Int. No. 1014-2023 and Int. No. 1024-2023.

With regard to the proposed language contained in File Int. No. 1024-2023, I would tell you that residential building security is only as good as the weakest component, which is usually humans. The principles of various assurance levels of physical and logical security using multi-factor authentication are well-captured in documents and standards published by the National Institute of Standards and Technology, or NIST.

The highest levels of assurance include biometrics as authentication factors. For buildings trying to offer highly-secure environments for their residents, all residents and guests should be required to enroll biometrically, or that high level of security can't be guaranteed. We do this in our businesses and enterprises, as well as in hospitals and healthcare facilities, and building owners should be allowed to offer this level of security to their tenants. This level of security isn't a threat to be restricted; rather, it is a privacy- and security-enhancing feature for residents and their guests.

In the broader commercial space, biometric technologies are useful in fighting crime and reducing theft. The ability for stores, shops and merchants to prevent shoplifting and robberies, or at least hold perpetrators accountable, is key to controlling this worrisome trend. According to a recent article in the *New York Times*, "Over the past five years, shoplifting complaints nearly doubled, peaking at nearly 64,000 last year, police data shows. Only about 34 percent resulted in arrests last year, compared with 60 percent in 2017."

Biometric technologies help in reducing crime, identifying repeat perpetrators, as well as facilitating loss prevention. When stores can't control their losses over time, they must make a difficult decision about whether they remain in business in that location or neighborhood. When stores and commerce flee from an area, that can create phenomena like "food deserts", limiting the options of area residents, which in turn exacerbates the cycle of crime and economic despair. Asking criminals for permission to enroll them biometrically isn't realistic and doesn't support the objective of reducing crime in New York City.

The bill language contained in File Int. No. 1014-2023 is equally as fraught with unintended consequences. If, for instance, the Council's intention is to punish Madison Square Garden and other places of business by denying them the use of biometric technology as a public venue, this bill, if enacted into law, will end up backfiring. It will not accomplish the intended punishment of the owner of Madison Square Garden for perceived bad (but not illegal) behavior, and you will deny the technology to less fortunate individuals and businesses for purposes that the citizens of New York would find beneficial.

Legislative efforts like these two bills are well-intentioned but could benefit from more expert input from organizations like the IBIA. However, it is impractical to think we can advise all of the state and local legislative bodies that are grappling with similar challenges. What has resulted is a patchwork of inconsistent state and local legislation that is complex and results in compliance difficulties, impedances to commerce — especially interstate commerce — and imposes unnecessary and burdensome costs for businesses whose points of presence and operations take place in and across many states. The IBIA believes this results in an unreasonable and preventable burden on businesses seeking to implement advancements involving biometrics and to comply with privacy laws.

Laws such as the Illinois Biometric Information Privacy Act, or 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. 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.

I urge you to support regulatory efforts at the federal level, and carefully reconsider what should be done locally. Biometric technologies should never be subject to bans, or there will be unintended consequences for commerce, convenience, and the security of our citizens.

Thank you, respectfully, for your time today. I can take questions if you wish.

# # #

IACSP
International Association of Certified Surveillance Professionals

STATEMENT OF

DERK BOSS

PRESIDENT

INTERNATIONAL ASSOCIATION of CERTIFIED SURVEILLANCE PROFESSIONALS

ON

BIOMETRIC RECOGNITION TECHNOLOGY

BEFORE THE

COMMITTEE ON CIVIL AND HUMAN RIGHTS

AND THE

COMMITTEE ON TECHNOLOGY

THE NEW YORK CITY COUNCIL

MAY 3, 2023

IACSP
International Association of Certified Surveillance Professionals

Madam Chair and Members of the City Council, I am pleased to present testimony regarding legislation making it unlawful for any place of public accommodation to use facial recognition technology to identify a customer and to require written consent before any biometric recognition technology could be used. We have serious concerns that City Council efforts to prohibit or limit the use of biometric recognition technology will make businesses less efficient and less safe. We would like to work with the council to shape future constructive regulations in this area.

My name is Derk Boss. I'm Director of Surveillance at Angel of the Winds Casino Resort and I serve as President of the International Society of Certified Surveillance Professionals (IACSP). IACSP was created in 2001 with the primary objective of training surveillance personnel. We provide affordable training and have developed a professional certification program, the Certified Surveillance Professional (CSP).

When we began the IACSP over twenty years ago, our primary focus was training members for surveillance methodology, internal theft and fraud, and casino games protection. Over the years we added risk and liability training, and then about twelve years ago, training programs in Homeland Security and Emergency Response. Our training courses have served our membership well. Indeed, the CSP certification has become a recognized standard throughout our industry.

At the outset, we acknowledge people have raised equal protection concerns and criticisms of algorithmic bias that misidentify some minorities. We submit that there is less chance of racial discrimination with Facial Recognition Technology (RFT) compared to when a human element is introduced. AI engines are the backbone of the facial recognition process, powering the algorithm that matches a live image to a face template in the database to determine how likely it is that one image is the same as the other. FRT is machine-driven, it is not subjective like security guard wanding or other measures where racial bias may creep in.

As discussed in more detail below, the National Institute of Standards and Technology (NIST) found that FRT accuracy had improved dramatically and that more accurate systems were less likely to make errors based on race or gender. The algorithm at the heart of the system, the application that uses it, and the data it's fed all play a role. Moreover, the quality of cameras and photos used with facial recognition systems are constantly upgraded.

IACSP's background and member focus make us well qualified to discuss the legislation before the City Council today. While we understand the concerns about the potential risks and misuses of biometric technology, we believe that the legislation discussed today is overly broad.

File #: 2023-3301 by Council Members Hanif and Gutierrez prohibits any provider of public accommodation from using biometric recognition technology to verify or identify a customer. File #: 2023-3300 by Council Members Rivera, Sanchez and Caban would ban owners of residential buildings from installing, activating, or using biometric recognition technology to identify tenants or their guests.

Both approaches place a city-wide restriction on the use of biometric recognition technology and will thwart legitimate uses of facial recognition technology.

More specifically, the legislation is problematic because it would roll back three primary beneficial uses of the technology.

1. The use of facial recognition technology is an efficient tool for security to help identify bad actors or other persons of interest.

2. Businesses can be more efficient implementing credentialing processes by using biometric recognition technology.

3. The use of biometric technology at events and entertainment venues improves the customer experience and makes it easier to enter a space. In a fast-paced and technology- savvy society, customers demand innovations that enhance the value of their experience.

The findings outlined above, and discussed in more detail below, suggest that that the City Council should tread cautiously when seeking to place restrictions on FRT.

EFFICIENT SECURITY TOOL

FRT is used to enhance public safety at large events by monitoring people entering and identifying individuals who are banned or not allowed in, mitigating security issues at the entrances. This enables security and law enforcement to proactively be alerted to safety concerns. FRT has revolutionized security and law enforcement over the years. With powerful AI engines, the speed and accuracy of matching suspects in criminal investigations and locating lost persons has improved dramatically.

Securing a city like New York is a major challenge, particularly given the city's status as a target for terrorism and other threats. FRT is one tool that can improve public safety and enhance security efforts.

How many of you unlock your iPhones by looking at a screen? Today, we use FRT and other biometric technologies and people not only accept these approaches, but they also rely upon them. DNA technology identifies the bad guys and holds people responsible for their actions. Fingerprinting technology provides the same benefits. These are not “scary” technologies that are flagged for racial bias. It is important to consider FRT in the same family of tools that are already proven and serve the common good.

BUSINESS SECURITY EFFICIENCIES

Businesses implementing biometric access control systems gain efficiencies after initial set-up. In cases where traditional methods of identification, such as RFID cards, have proven to be inadequate or easily circumvented, FRT can provide a more secure and reliable method of identifying individuals and ensuring that only authorized personnel are granted access. Secondarily, a cardless security system is good for the environment due to the reduction in plastics usage and associated costs.

IMPROVED CUSTOMER EXPERIENCE

This use of biometric technology can help New York City businesses improve their operations and provide a better experience for customers. With your face, fingerprint, or other identifier a person's identity can be quickly verified and allows entry without a ticket. Airports and sporting venues use the technology so customers can avoid long lines. That is, many people are choosing FRT rather than waiting at an airport's Transportation Security Administration (TSA) scanning gate.

Retailers use FRT to personalize the shopping experience for customers, such as by recognizing past purchases and providing tailored recommendations. Personalization allows the experience to be more secure and unique. Without some way to know who people are when they arrive there is not another way to tailor the experience. Customers are becoming increasingly comfortable with these technology innovations. The technology can also be used to reduce fraud and theft, helping businesses to protect their assets and improve their bottom line.

Apart from retail applications, FRT can identify those banned or self-excluded from casinos. Many IACSP members come from the casino industry. The primary use of FRT in casinos today is to keep bad actors out while welcoming valued patrons. The fact is that even if someone is banned or self-excluded, they may still come back to the venue. Operators need to be able to recognize those individuals and detect them before they can cause further issues. FRT can also identify a casino's most valued patrons. When a VIP arrives, FRT allows the venue to assign a host and tailor the entertainment experience.

RELIABILITY OF FACIAL RECOGNITION TECHNOLOGY

In addition to the strong public policy reasons to not hamper FRT, there are strong scientific underpinnings to the technology. FRT has been pulled into larger public debates about privacy, race, and law enforcement. These are hotly debated topics that sometimes create a confusing narrative. Regarding concerns about the potential risks and misuse of the technology, we believe it is important to consider the findings by the NIST when evaluating FRT to understand the accuracy and variance between algorithms. Advancements in AI technology continue to develop at a rapid rate. Like any new technology, improvements in FRT are iterative and error rates have fallen dramatically over the last five years.

NIST, a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce, has conducted multiple studies to evaluate the accuracy and performance of facial recognition algorithms from various developers. These studies involve testing the algorithms on large datasets of face images to evaluate how well they can perform specific tasks such as identification, verification, and one-to-many matching. NIST typically conducts facial recognition testing on an ongoing basis, with new studies and reports released periodically as needed, at least annually.

In September 2022 NIST's Ongoing Face Recognition Vendor Test (FRVT) found that face recognition accuracy has improved markedly due to the development of new recognition algorithms and approaches

(FRVT, Part 5, September 27, 2022). The current generation of facial recognition algorithms is more accurate than ever, and there is little to no evidence of racial bias in the algorithms themselves.

As noted earlier, AI engines power the algorithm that matches a live image to a face template in the database. The quality of cameras and photos used with facial recognition systems is critical to ensure a high level of confidence in matching. This can minimize the risk of inaccurate results and ensure that the technology is used in a responsible and equitable manner. These engines are trained on large datasets of face images, often collected from a diverse range of sources to ensure a variety of races, genders, and ages.

In addition to facial recognition, there are other biometric technologies that have been widely adopted and proven to be effective for identity verification. For example, DNA and fingerprint matching have been used for many years in law enforcement and forensics to identify suspects and solve crimes. Dental matching is also a common method used to identify people. From the moment we are born, we recognize faces and keep track of them in our minds. Biometric technologies are simply an extension of our natural ability to recognize and remember unique features that distinguish one person from another. Stopping the development and use of biometric recognition technology would require stopping the development of AI, and that is neither possible nor in the national interest.

SAFEGUARDS

We understand the City Council's desire to create a new legal or regulatory framework. Certainly, the use and regulation of biometric recognition technology may differ depending on commercial use, general government use, and law enforcement use. Our members are starting to examine new regulatory frameworks and guidelines including the appropriate level of transparency and how to notify the public that biometric recognition technology is being used. We are aware of some states and municipalities that have transparency requirements, including how to notify the public that biometric screening is being used. We believe this transparency could include annual reporting, public consultation, and making information publicly available on how biometric recognition technology is being used. It is simply not practical to require written consent before any biometric recognition technology is employed as proposed in File #: 2023-3301.

CONCLUSION

FRT can be an exceptionally useful tool for security and private businesses. We can look to other biometric technologies as evidence of the potential benefits of using such methods to verify identity. We oppose across-the-board restrictions on the use of FRT. Let's be clear--- such restrictions will negatively impact public safety and municipal operations.

IACSP understands concerns about technology advancement generally and, in this specific situation, concerns about the potential risks and misuses of the technology. However, we must recognize that facial recognition technology has countless benefits and can be used in a responsible and ethical manner. FRT continues to improve and is not subjective like humans. Moreover, IACSP works on the human side through our training programs and CSP certification. As a result of IACSP's work, the human element is done right. Our members are well-trained and knowledgeable.

For commercial and government uses other than law enforcement, people value the convenience and efficiency FRT provides, leading to increasing demand. Biometric recognition technology will continue to be developed and deployed because of the convenience for consumers and the benefits to public safety. Continued progress in sensors and AI will increase availability and performance of the technologies used for facial recognition.

As we continue to discuss possible regulation and oversight of facial recognition technology, it is essential that we take a balanced approach, weighing the potential benefits and risks in order to ensure the best possible outcomes for all New Yorkers. IACSP would like to serve as a resource to the council as new standards are developed. With proper regulation and oversight, we can ensure that the technology is used for the public good, and that concerns about privacy and civil liberties are addressed appropriately.

TESTIMONY REGARDING

Intro 1014-2023 and Intro 1024-2023

PRESENTED BEFORE:

THE NEW YORK CITY COUNCIL'S
COMMITTEE ON TECHNOLOGY AND
COMMITTEE ON CIVIL AND HUMAN RIGHTS

PRESENTED BY:

LISA MEEHAN
PRO BONO SCHOLAR
MOBILIZATION FOR JUSTICE, INC.

MAY 3, 2023

MOBILIZATION FOR JUSTICE, INC.
100 William Street, 6th Floor
New York, NY 10038
(212) 417-3700
www.mobilizationforjustice.org

1. Introduction

Mobilization for Justice's (MFJ) mission is to achieve justice for all. MFJ prioritizes the needs of people who are low-income, disenfranchised, or have disabilities as they struggle to overcome the effects of social injustice and systemic racism. We provide the highest-quality free, direct civil legal assistance, conduct community education and build partnerships, engage in policy advocacy, and bring impact litigation. MFJ also promotes diversity, equity, and inclusion in our workplace, and understands the need to eliminate all racial disparities to achieve justice for all.

MFJ appreciates the opportunity to share with the New York City Council Committee on Technology and Committee on Civil and Human Rights on our thoughts about limiting the use of biometric recognition technology, particularly Facial Recognition Technology (referred to hereafter as "FRT"), by providers of public accommodations and by landlords of residential apartment buildings. We believe that landlords install FRT under the guise of security, but that its installation and use serve to surveil and harass tenants, particularly those who are marginalized and already at risk of being displaced. We support the passage of initiative 1014-2023 to protect the privacy of all New Yorkers, and we support the passage of initiative 1024-2023 to protect tenants' right to stay in their homes and live free from surveillance.

2. Facial recognition and surveillance are rooted in a history of racism.

Facial recognition is rooted in a long history of racism and classism. It dates back to New York State's "Lantern Law", passed in 1713, which forced Black, Indigenous, and mixed-race people walking after dark to carry a lantern illuminating their faces, so that they would be visible and identifiable to white authorities.[1] This culture of surveilling and criminalizing Black and brown communities only morphed as technology improved. Authorities have long used crime and security as justifications for surveillance, including installing high-intensity lighting in Black and brown neighborhoods.[2] The security justifications for installing FRT should be viewed in the same light.

3. The public does not support landlords' use of FRT.

The use of FRT does not have widespread support among average Americans. In 2019, Pew Research Center polled U.S. adults on their opinions on whether apartment building landlords using facial recognition technology to track who enters and leaves their building is acceptable. Only 36% of respondents thought it was acceptable.[3] Another recent study indicates that 65% of Americans would want the choice to opt out of FRT used in retail stores – this percentage would likely be the same, if not higher, for opting out of FRT used by landlords.[4]

---

[1] Erin McElroy & Manon Vergerio, *Automating gentrification: Landlord technologies and housing justice organizing in New York City homes*, SOCIETY AND SPACE, 40(4), 607-626 (2002).
[2] Id.
[3] Aaron Smith, *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, PEW RESEARCH CENTER (Sept. 5, 2019) at https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/.
[4] NYCLU Testimony before the New York City Department of Consumer and Worker Protection regarding the new rules to implement Local Law 3 of 2021; August 30, 2020.

Despite the widespread use of FRT (a Georgetown Law study estimated that as many as 1 in 2 Americans have had their photos searched by law enforcement using FRT on driver's license databases[5]), it is not widely accepted or understood. FRT's use, particularly in settings like apartment buildings where individuals lack a real choice to decline its use, is particularly problematic.

4. Landlords already use other types of technology to surveil, displace, and deregulate apartments.

Landlords already use a wide range of technology to surveil tenants. Security cameras have already been found to be a tool for harassment.[6] As biometric surveillance becomes more widespread there is no reason to believe that it will not be used for similar purposes. For example, Atlantic Plaza Towers, which proposed installing FRT until it was ultimately stopped by tenants, has long used an extensive camera network to film tenants. There are security cameras that watch the exterior of the building, the doorways, the elevators, and the hallways – practically everywhere besides in tenants' actual apartments.[7] When tenants tried to inform their neighbors of the upcoming changes, the five tenants working to organize their building were sent a notice from their property manager with their pictures included warning them to stop despite tenant organizing being a legally protected activity.[8]

An even more alarming example is Teman GateGuard, an "AI Doorman" that has been installed in approximately 1,000 residential buildings across New York City. Teman advertises GateGuard as a tool to deregulate apartments by catching illegal sublets or other lease violations. Teman's sales team emailed customers to "use GateGuard AI Doorman Intercom to catch illegal sublets, non-primaries, and Airbnbs so you can vacate a unit" to allow landlords to "combine a $950/month studio and a $1400/month one-bedroom into a $4200 DEREGULATED two-bedroom." Teman boasted on LinkedIn that GateGuard had been used to evict tenants from over 600 rent-stabilized units from 2016 to 2018.[9]

5. Landlords already use FRT to surveil and evict tenants, and ultimately gentrify neighborhoods.

Landlords across New York City are already using FRT. FRT is loosely regulated, so it is difficult to say just how widespread landlords' use of it is. There is no formal registry of

---

[5] Lindsay Barrett, *Ban Facial Recognition Technologies for Children and for Everyone Else*, BOSTON UNIVERSITY JOURNAL OF SCIENCE AND TECHNOLOGY LAW, 26(2), 223-285 (2020).

[6] See, e.g., Suchdev v. Grunbaum, 202 A.D.3d 1126 (2d Dep't 2022 (SRO tenants being monitored by over 20 cameras in a small building); Martinez v. Ling, 2021 NYLJ Lexis 72 (Civ. Ct. Queens Cty.) (Camera part of pattern of harassment used to force out a Spanish-speaking tenant so the apartment could be demolished and deregulated).

[7] Erin Durkin, *New York tenants fight as landlords embrace facial recognition cameras*, THE GUARDIAN (May 30, 2019) at https://www.theguardian.com/cities/2019/may/29/new-york-facial-recognition-cameras-apartment-complex#:~:text=New%20York%20tenants%20fight%20as%20landlords%20embrace%20facial%20recognition%20cameras,-More%20than%20130&text=Tenants%20in%20a%20New%20York,affront%20to%20their%20privacy%20rights.

[8] Ginia Bellafante, *The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?*, NEW YORK TIMES (Mar. 31, 2019) at https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html.

[9] McElroy & Vergerio, supra note 1, at 607-626.

"property technology" companies, or "proptech." The databases that do exist, such as Unissu[10], do not include every technology company used by New York landlords (for example, the FRT company proposed in the Atlantic Plaza Towers, Stonelock, does not appear on Unissu's database). Landlords are also not required to notify any agency when they install new technology, so there are no formal records of which buildings are utilizing which technology. Tenant organizers have created a website called Landlord Tech Watch, where tenants can submit information about the technology used by their landlords. Landlord Tech Watch has identified nine different buildings in New York City already using FRT, but there are likely many more.[11]

Landlords will often justify installing FRT to increase security, but this is not a convincing justification to many tenants, who instead see it as a surveillance and gentrification effort.[12] The installation of FRT in buildings often coincides with the gentrification of those areas. Taino Towers, a federal public housing complex in East Harlem, had FST21 SafeRise FRT installed in 2013. Four years later, the city upzoned the area for new development.[13] Knickerbocker Village, an affordable housing apartment complex in the Lower East Side with mostly Asian-American immigrant residents, also installed FST21 FRT at the same time that the area was slated for construction of a new luxury development, Extell's One Manhattan Square.[14] Morris Avenue Apartments in the Bronx, which includes 35 units for families coming out of homeless shelters, also installed Reliant Safety FRT.[15]

Tenants in the Atlantic Plaza Towers in East New York successfully stopped their landlord from installing FRT in a high-profile legal battle. Atlantic Plaza Towers' area of East New York had been upzoned in 2014, intended to pave the way for new development. The neighborhood is also the most surveilled neighborhood in all of New York City, with 577 NYPD cameras in less than two square miles. Tenants in Atlantic Plaza Towers were already subjected to video surveillance by CCTV cameras that their landlord used to catch minor lease violations and curb tenant organizing. It was against this backdrop that the landlord of Atlantic Plaza Towers proposed the installation of Stonelock FRT.[16]

The Atlantic Plaza Towers tenants saw FRT as the new frontier of their landlord's efforts to surveil them, violate their privacy, and ultimately oust them from their homes. As one Atlantic Plaza tenant put it, "we as residents do not want to feel as though we are prisoners, tagged and monitored as soon as we make a move... we have experienced disrespect, and have been continuously treated like criminals in our own homes … our biggest danger is that this technology will get into the hands of third-party entities, who will get unsolicited access to our biometric information, and ultimately we will be placed in damaging systems such as perpetual police lineups."[17] The residents felt that the proposal "had less to do with improving their own

---

[10] https://www.unissu.com/proptech-companies?ordering=1
[11] https://antievictionmappingproject.github.io/landlordtech/
[12] Durkin, supra note 7.
[13] McElroy & Vergerio, supra note 1, at 607-626.
[14] Id.
[15] Id.
[16] Id.
[17] Id.

security, and more with attracting new tenants to the buildings in an area of Brooklyn primed for gentrification.“ “He doesn’t want Spanish. He doesn’t want Black. He wants white people to come into the neighborhood,” said another tenant.[18]

Because there is already documented evidence of landlords using various types of technology, including FRT, to displace tenants, it is safe to assume that allowing the further proliferation of this technology will continue to harm tenants, particularly those who are already at risk of being displaced and evicted unless reasonable regulations are enacted.

6. FRT is less accurate for historically marginalized populations, which results in less, not more, security for residents after its installation.

It is well-documented that FRT is less accurate at identifying faces of people of color[19], women[20], elderly people[21], children[22], and transgender and non-binary people[23] than it is at identifying faces of cisgender white men. Software is particularly inaccurate at identifying the faces of women of color, with inaccuracy rates as high as 46.8%.[24] Even elected officials are not safe from misidentification. When the ACLU ran the faces of every member of Congress through Amazon’s Rekognition software, it identified 28 members of Congress as other people with criminal records. The software’s misidentification rates were disproportionately high among the Black members of Congress: nearly 40 percent of Rekognition’s false matches in the test were people of color, even though they make up only 20 percent of Congress.[25]

This results in major issues for tenants when FRT misidentifies them. In Knickerbocker Village, tenants report that the FRT cameras often don’t work, particularly when sunlight hits them directly or when it is dark. So, people have to resort to humiliating dances in front of the

---

[18] Durkin, supra note 7.

[19] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy: Disparities in Commercial Gender Classification,* 81 PROCEEDINGS OF MACHINE LEARNING RESEARCH 1, 2-8 (Feb. 2018). See also, Raji & Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products,* CONFERENCE ON ARTIFICIAL INTELLIGENCE, ETHICS, AND SOCIETY 1- 5 (2019); Joy Buolamwini, *When the Robot Doesn't See Dark Skin,* NEW YORK TIMES (June 21, 2018), at https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html.

[20] See Buolamwini & Gebru, supra note 19, at 6, 8, 10; Raji & Buolamwini, , supra note 19, at 4; Buolamwini, *supra* note 19.

[21] Patrick J. Grother, Mei L. Ngan, and Kayeek K. Hanaoka, *Face Recognition Vender Test Part 3: Demographic Effects*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY REPORT 8280 (Dec. 2019), at https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects.

[22] Id.

[23] Os Keyes, *The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition,* 2 PROCEEDINGS OF THE ACM ON HUMAN-COMPUTER INTERACTION 1, 4 (2019).

[24] Larry Hardesty, *Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence* Systems, MIT NEWS (Feb. 11, 2018) at https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212. In this study, researchers created an evenly representative data set of over 1,200 faces. They classified skin tone using the dermatologist-created Fitzpatrick scale (which scales on a range of 1 to 6). They applied three commercial facial-analysis systems from major technology companies to the data set. For the darkest skinned women (6 on the Fitzpatrick scale), the average error rate across the three softwares tested was 46.8%.

[25] Mutale Nkonde, *Automated Anti-Blackness: Facial Recognition in Brooklyn, New York*, HARVARD KENNEDY SCHOOL JOURNAL OF AFRICAN AMERICAN POLICY, Vo. 2019-20, 30-36 (2019).

cameras just to be "seen." Often guards end up buzzing everyone who is waiting for the cameras into the building without checking who is coming in. This results in less security than a traditional key or fob setup.[26] The cameras at Knickerbocker Village also come up with false positive matches. One tenant's cousin, who is Asian-American, was let in by the FRT cameras even though she did not live there. The technology mistakenly matched her face with the face of a tenant who lived there (70% of the building's tenants are Asian-American).[27] Via both false negative and false positive identifications, using FRT to allow access to buildings creates less safety and security for tenants, despite landlords' marketing otherwise.

7. FRT invades people's privacy.

Even if FRT were able to identify all faces with perfect accuracy, its use is still a violation of tenants' privacy and is not justifiable. FRT instills a culture of surveillance and violates our basic personal privacy and right to be anonymous in public space. With FRT, we can no longer be a face in the crowd. When FRT is deployed by landlords, "your work life, your love life, your family life, your religious life – all of that is opened up for display to people using facial recognition to track your comings and goings from the building."[28] Furthermore, it is dehumanizing. In the words of Icemae Downes, who lives in Atlantic Plaza Towers, "We do not want to be tagged like animals. We are not animals. We should be able to freely come in and out of our development without you tracking every movement."[29]

New York State Division of Housing and Community Renewal (DHCR) has already stopped landlords from installing similarly invasive biometric identification systems in buildings because the privacy concerns outweighed any added security benefit from the system.[30] The commissioner of DHCR stopped one landlord from installing a fingerprint scanner. It found that "tenants of a building utilizing a biometric entry system are required to share an extensive amount of personal information, identifying characteristics, and/or location data," and that the landlord had "failed to show that any safeguards exist to protect against abuses of tenant privacy or preclude the sharing such information with third parties."[31] The privacy implications of FRT could be even more severe than other kinds of biometric tracking systems, and the technology should be treated with even more caution.

Tenants in New York City also have a right to associate with whom they please, and FRT infringes upon that right. This ties into our most basic fundamental rights to privacy and freedom of association under the First Amendment of the Constitution. Tenants are supposed to be allowed to invite guests to their home, as well as live with and visit with their family members in their home. They are supposed to be able to have service workers come to their homes, such as home health aides, childcare workers, and others. Forcing every guest to register with FRT and be subject to surveillance is unjustifiable. This is also a situation that is forced onto renters.

---

[26] McElroy & Vergerio, supra note 1, at 607-626.
[27] Id.
[28] Durkin, supra note 7.
[29] Id.
[30] In the Matter of Rangoon, Inc., Administrative Review Docket # GO410031RO.
[31] Id.

Homeowners have the choice as to whether to install technology (*e.g.*, Ring cameras) on their homes, whereas renters are deprived of that choice when their landlords unilaterally decide to install this technology. The installation of FRT deprives both tenants and their guests of their agency and privacy.

8. Other jurisdictions have enacted or are considering bans on facial recognition technology.

We urge the Council to adopt the proposed bills to implement further limitations on FRT. New York City would not be the first jurisdiction to recognize and take action against FRT due to the myriad issues associated with the technology.

There are a number of jurisdictions that have passed bans on government use of FRT. San Francisco, CA[32], Somerville, MA[33], Baltimore, MD[34], Boston, MA[35], Oakland, CA[36], and Berkeley, CA[37] have all banned city government use of the technology; New York State passed a two-year moratorium on the use of FRT in schools[38]; and California passed a three-year ban on the use of FRT on body camera footage[39]. Legislation has also been proposed at the federal level: Senators Cory Booker and Jeff Merkley have introduced a bill to Congress that would ban the use of FRT by the federal government until it is better regulated[40].

---

[32] Kate Conger, Richard Fausset, and Serge F. Kovaleski, *San Francisco Bans Facial Recognition Technology*, NEW YORK TIMES (May 14, 2019), at https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.
[33] Katie Lannan, *Somerville Bans Government Use of Facial Recognition Tech*, WBUR (Jun. 28, 2019), at https://www.wbur.org/news/2019/06/28/somerville-bans-government-use-of-facial-recognition-tech.
[34] Joseph J. Lazzarotti, et. al., *City of Baltimore May Criminalize the Use of Facial Recognition Technologies by Businesses*, NATIONAL LAW REVIEW (Jun. 21, 2021) at https://www.natlawreview.com/article/city-baltimore-may-criminalize-use-facial-recognition-technologies-businesses.
[35] Ally Jarmanning, *Boston Lawmakers Vote to Ban Use of Facial Recognition Technology By The City*, WBUR (Jun. 24, 2020) at https://www.npr.org/sections/live-updates-protests-for-racial-justice/2020/06/24/883107627/boston-lawmakers-vote-to-ban-use-of-facial-recognition-technology-by-the-city.
[36] Sarah Ravani, *Oakland Bans Use of Facial Recognition, Citing Bias Concerns*, SAN FRANCISCO CHRONICLE (Jul 16, 2019), at https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php#:~:text=The%20Oakland%20City%20Council%20voted,San%20Francisco%20and%20Somerville%2C%20Mass.
[37] Sara Merken, *Berkeley Bans Government Face Recognition Use, Joining Other Cities*, BLOOMBERG LAW (Oct. 16, 2019), at https://news.bloomberglaw.com/privacy-and-data-security/hold-berkeley-bans-government-face-recognition-use-joining-other-cities.
[38] Juan Miguel & Daniel Schwarz, *NY is Ignoring the Ban on Facial Recognition in Schools*, NYCLU (Jun. 28, 2022), at https://www.nyclu.org/en/news/ny-ignoring-ban-facial-recognition-schools#:~:text=State%20officials%20are%20disregarding%20the%20law%20and%20putting%20students%20in%20danger.&text=To%20protect%20students%2C%20New%20York,destroying%20biometric%20surveillance%20in%20schools.
[39] Katy Stegall, *3-Year Ban on Police Use of Facial Recognition Technology in California to Start in the New Year*, SAN DIEGO UNION-TRIBUNE (Dec. 20, 2019), at https://www.sandiegouniontribune.com/news/public-safety/story/2019-12-20/3-year-ban-on-police-use-of-facial-recognition-technology-in-california-to-start-in-the-new-year
[40] Rebecca Heilweil, *How a Basic iPhone Feature Scared a Senator into Proposing a Facial Recognition Moratorium*, VOX (Feb. 19, 2020), at https://www.vox.com/recode/2020/2/19/21140503/facial-recognition-jeff-merkley-regulation-clearview-ai.

Portland, Oregon's city council recently enacted the farthest-reaching ban in the country, which bans private businesses from using FRT. The Portland City Council emphasized that residents and visitors should be able to use public spaces without violating their personal privacy and anonymity, and that the technology poses a particular risk to communities who have been subject to over-surveillance. Companies may be required to pay $1000 for each day they violate Portland's ban.[41]

9. Conclusion

MFJ urges the City Council to pass initiatives 1014-2023 and 1024-2023 to protect New York City residents – and in particular, low-income and marginalized tenants who are at particular risk of being harmed by the use of biometric recognition technology and FRT. The technology will only grow more pervasive unless NYC joins other progressive communities in protecting privacy and respecting the rights of renters.

[41] Alfred Ng, *Portland, Oregon, Passes Toughest Ban on Facial Recognition in US*, CNET (Sept. 10, 2020), at https://www.cnet.com/news/politics/portland-passes-the-toughest-ban-on-facial-recognition-in-the-us/.

My name is Avi Kaner. I am an owner of the Morton Williams Supermarket chain, with stores primarily in Manhattan. We employ over 1,000 full time union employees. Our stores stayed open 24/7 during the Covid crisis as people were either hunkered down in their apartments or fleeing the city. Since then, our stores have been under assault by theft, driven directly by New York City's refusal to prosecute thieves. Stealing up to $1,000 at a time is now an entitlement in New York City. Just like many drug stores have shuttered their stores, supermarkets are now doing the same. We must have a way to protect ourselves from going out of business.

In the past, we would take polaroid photos of thieves and scotch tape them by the time clocks, so employees could recognize the thieves if they enter the supermarket again. There is no difference between that and using facial recognition. If a thief is caught on camera wiping out an entire section of the supermarket, we must have the ability to prevent that thief from coming into our supermarket again.

Over the past year, our gross margins are down 2% due to theft and the city's refusal to prosecute thieves. Additionally we have spent over $1 million a year on NYPD off-duty officers to post at the exits. This has practically wiped out any profit we have and threatens to shut down a number of our stores.

The city has done enough with its assault on businesses like ours. Many of our employees have been violently attacked when they tried to stop thieves, and the police refuse to arrest the thieves since the prosecutor will not prosecute them. We must have the ability to protect our businesses. We are not collecting biometric data. We are simply using photos of known thieves to prevent their entry into our stores.

I implore you to reject this misguided law, and instead protect the city's businesses, residents and employees.

Avi Kaner
avikaner@mortonwilliams.com
1-917-612-3494

May 3, 2022

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. 1014-2023

Thank you, Chairs Gutierrez and Williams 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 Intro. 1014 in "relation to prohibiting places or providers of public accommodation from using biometric recognition technology and protecting any biometric identifier information collected."

Intro. 1014, 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 both 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.

ACLU of New York

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

Testimony of Daniel Schwarz

On Behalf of the New York Civil Liberties Union

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

May 3, 2023

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

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

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

Biometric Surveillance Has No Place in New York City

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

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

---

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

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

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

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

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

Biometric Surveillance by Law Enforcement

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

[13] *Id.*

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The NYCLU supports this legislation and urges its passage.

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

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

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

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

Conclusion

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

PARTNERSHIP for New York City

Testimony of the Partnership for New York City

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

Int. 1014-2023

May 3, 2023

Thank you, Chairs Gutiérrez and Williams and members of the committees, for the opportunity to testify on Int. 1014 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 private sector employers of more than one million New Yorkers. We work together with government, labor, and the nonprofit sector to maintain the city's position as the preeminent global center of commerce, innovation, and economic opportunity.

The Partnership supports sensible safeguards for consumers around the use of biometric information but opposes Int. 1014 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. 1014 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. 1014:

- **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. 1014 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. 1014

- 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 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 1014-2023

New York City Council

Committees on Technology and Civil & Human Rights

May 3, 2023

Testimony Submitted by:

Kelsey Dorado

Director of State and Local Government Relations

Retail Council of New York State

kelseydorado@rcnys.com

RETAIL COUNCIL OF NEW YORK STATE
RESULTS FOR TODAY'S RETAILERS

Chairs Gutiérrez and Williams and Honorable Committee Members:

Good afternoon. My name is Kelsey Dorado, and 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 1014-2023.

As currently drafted, the 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."

We respectfully submit our opposition to this proposal, as it would prohibit a retail establishment from using certain technology to further address organized retail crime incidents in the five boroughs.

The Retail Council of New York State, on behalf of thousands of retailers, continues to prioritize the safety of employees and customers. According to the 2022 Retail Security Survey, eight in 10 retailers reported that violence and aggression associated with organized retail crime incidents increased in 2021. This is compounded by the fact that retailers, on average, experienced a 26.5% increase in organized retail crime incidents in the same year. This is a real and significant issue that must be addressed in a strategic manner, and it involves the sharing of information among victims of property theft, the New York Police Department and prosecutors.

In addition, the legislation would require retailers of all sizes to obtain the written consent of every customer in advance of any collection of biometric identifying information. In practice, this would completely disrupt the flow of commerce in the City of New York, as merchants with basic video or photo cameras would need to obtain written consent of each customer before they entered the store. This would be an impossible task for retailers, who strive to make the in-person shopping experience pleasant and accommodating.

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
Director of State and Local Government Relations
Retail Council of New York State
kelseydorado@rcnys.com

May 3, 2023

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

The Honorable Natasha Williams
Chair
Committee on Civil and Human Rights
New York City Council
New York, NY

Written Testimony of SIA for Hearing on The Use of Biometric Identification Systems in New York City

Dear Chair Gutiérrez, Chair Williams and Members of the Committees:

On behalf of Security Industry Association (SIA), a nonprofit trade association representing more than 70 companies headquartered in New York State and 1,300 nationwide, I appreciate the opportunity to participate in today's hearing. Our members provide a broad range of security and life safety products and services in the U.S and throughout New York. Among them are the leading developers 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 polices that would help ensure responsible and effective use of such technologies,[1] we have serious concerns with the two proposals relating to biometric technologies under consideration by the committees today.

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

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

- App-based accounts and payment systems utilizing biometric customer authentication on electronic devices.

[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/

- Customer choice of biometrics as a more convenient form of payment and access at sporting events and other entertainment venues.
- Biometrically-secured driver authentication for ride-share services.
- Convenient fingerprint or face access provided to gym members.
- Use of increasingly popular "virtual" or "remote" doorman systems by homeowners' associations and for residential buildings, which offers a more secure and convenient access for residents.
- Use of fingerprint time-clocks and cash register locks by business employees.
- Biometrically-secured building and door access control systems for workers.
- Biometrically-secured user authentication for account access and payment to a business, whether online or in-person.
- Biometrically-enabled security systems protecting persons or property, including systems augmenting efforts fight organized retail crime (ORC).
- Use of biometrics for streamlined embarkation on cruise ships, and seamless "curb-to-gate" air travel.

The prohibition on using biometric technologies would be applicable to a wider range of businesses than New York City's existing biometric data ordinance, covering any "place or provider of public accommodation." Many businesses will undoubtedly be caught unaware, and subjected to litigation 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 technical violations (versus actual 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 use of biometric technologies but uses a similar enforcement mechanism for archaic 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 alleging "consumer harm" have included the use of virtual try-on services, and 40% have involved security and identity verification services.[2]

Additionally, we are concerned that the proposals appear to modify existing ordinances to expand 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 are imposed on businesses collecting biometric identifier information "of any person." This is not limited to persons located in New York City and appears to also include employees.

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

We are further concerned that some policy discussions regarding biometric technologies have been driven by misconceptions about the nature and security of biometric data. Biometric technologies actually play a key role in protecting privacy during transactions that require identity verification, by preventing exposure of personal information (date of birth, Social Security Number, address, etc.) that is far more vulnerable to compromise and abuse. Biometric technologies create a numerical "template" based on an individual's biological characteristics to compare with a template or templates already enrolled in a database or on a device. This numerical string of data is created and readable only within that specific software. Outside and apart from the software, this template by itself does not contain any personally identifiable information. Importantly, it cannot be used to re-create the image (of a fingerprint, face, etc.) that it was derived from. Each provider uses a different process to create and compare templates unique to that proprietary system. A template created in one system cannot be used in another.

In this way, the use of mathematical vectors acts as secure cryptography for biometric data, preventing identity hacking even if that data is stolen, and naturally serves to limit unauthorized use by third parties. While such data would be useless if sold or shared, its collection, storage and processing can easily be optimized to ensure privacy and security using encryption and other cybersecurity and privacy best practices in protecting other forms of sensitive information.

In contrast to the blanket bans proposed, a measured approach could address specific concerns about biometric identification technologies. SIA and its members strongly support the responsible use of these technologies, and we stand ready to provide any additional information or expertise needed as you consider related issues.

Respectfully,

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

SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

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

STATEMENT OF
ALBERT FOX CAHN, EXECUTIVE DIRECTOR
AND NINA LOSHKAJIAN, LEGAL FELLOW
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT ("S.T.O.P.")

BEFORE THE COMMITTEE ON TECHNOLOGY,
NEW YORK CITY COUNCIL

FOR AN OVERSIGHT HEARING ON THE USE OF
BIOMETRIC IDENTIFICATION SYSTEMS IN NEW YORK CITY

PRESENTED
May 3rd, 2023

Good afternoon, Chair Gutiérrez, Chair Williams, and members of the Committees on Technology and Civil and Human Rights. 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. Thank you for organizing this important hearing. We appreciate the opportunity to testify today on the harms of biometric surveillance. We urge the Council to pass Intros 1014 and 1024, and to support the introduction of a ban on government use of facial recognition technology (FRT).

I. Biometric Surveillance is Harmful and Discriminatory

FRT is biased and error prone. FRT 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. Numerous people, disproportionately Black, are wrongly arrested after being misidentified through facial recognition.[2]

Human bias infects A.I. systems. If a security camera learns who is "suspicious looking" using pictures of inmates, the A.I. replicates human bias and discrimination. When facial recognition software can only recognize two genders, we leave transgender and non-binary individuals susceptible to misidentification and wrongful arrest.[3] 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.[4]

Further, allowing businesses and landlords to collect biometric information makes them an even more lucrative target for identity thieves and hackers.[5] 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.[6] More dangerous than other personal identifiers like a social security number, biometric

---

[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, *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.
[4] 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.
[5] *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.
[6] 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.

identifiers are static and are almost impossible to change.[7] When a hacker acquires another person's biometric data, it puts them at risk for identity theft for the rest of their lives.[8]

II. Intros 1014 and 1024

Given the bias, invasiveness, and potential for abuse of FRT, it has no place in New York businesses. And yet it does. New Yorkers should not be forced to accept biometric surveillance as part of simple activities like buying groceries or taking their kids to a baseball game. Yet this is the reality in our city, and it will continue to be until the Council passes this important legislation. Last year, the Mets implemented a facial recognition ticketing system at Citi Field.[9] In partnership with Wicket, a computer vision company, the Mets are encouraging fans to upload selfies on MLB.com to register their faces and then check-in at the gates. The Mets have touted this system as a new high-tech amenity. But FRT is not an amenity, it is discriminatory surveillance. And it is far from high-tech, as it often struggles to identify faces when people are wearing hats, seemingly an obvious issue for fans headed to a baseball game.[10]

James Dolan, the owner of Madison Square Garden Entertainment Corporation (MSG), has faced scrutiny for his use of FRT at the company's venues, including from New York State Senators[11] and Attorney General James.[12] Dolan has used the incredible power of FRT to seek vengeance against MSG's foes, blocking access to ticketholders who are affiliated with law firms involved in pending lawsuits against MSG. In one case, this meant ejecting a mother trying to watch the Rockettes show at Radio City Music Hall with her daughter's Girl Scouts troop.[13] 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. Many of the most popular venues in NYC, owned by MSG, now deploy FRT, and the technology is already used in some grocery stores.[14] Stores like Brooklyn Fare and Westside Market may be scanning the face of every single customer walking through their stores and storing that sensitive personal data indefinitely.

---

[7] 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/.

[8] *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.

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

[10] 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.

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

[12] 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.

[13] 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/

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

Intro 1014 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 FRT 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.

Similarly, use of FRT and other biometric surveillance technologies in residential settings opens tenants to harassment, discriminatory eviction, and compromises their privacy. 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 FRT and successfully prevented the plan from proceeding.[15] Their organizing highlighted the disproportionate impact of the use of these biometric security systems in low-income communities of color.[16]

The racial bias of FRT 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.[17] To protect immigrant communities in our city, we cannot let landlords have access to residents' biometric data.

Intro 1024 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. The bill should be strengthened through amendments creating a strong private right of action applicable to all provisions, not just sale, with statutory damages and punitive damages, but its passage is critically important to make New Yorkers safer in their homes.

III. The Need for Additional Legislation

While we are heartened to see the introduction of these two bills, we are disappointed that the Council has seemingly ignored the growing threat from 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 FRT, but the Council has not even introduced a bill yet or included it on any committee agenda.

This is an urgent issue. New York Police Department (NYPD) officers reported in open-records litigation that the department used FRT more than 22,000 times in just three years. Officers use

---

[15] 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.

[16] *Id.*

[17] *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.

pseudoscientific tactics that exacerbate the risk of error, such as running scans of celebrity lookalikes.[18] The Georgetown Law Center on Privacy and Technology documented the kinds of abuses that are "common practice" at NYPD.[19] 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."[20]

Police also abuses FRT to surveil protestors. There are reports that the NYPD used FRT to target Derrick Ingram for his leadership of a peaceful Black Lives Matter protest. Police later surrounded Derrick's home with more than 50 officers as part of a retaliatory raid.[21]

Facial recognition searches are also skewed by where surveillance cameras are placed in our city. The technology is misused in a way that further replicates historical biased policing, with disproportionately high placement of cameras in low-income communities of color.[22]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."[23]

Because of its documented biases and its replication of historically flawed police practices, FRT should not be used by the NYPD or any other government agency. 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.[24]

Thank you for the opportunity to testify today.

---

[18] 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.
[19] 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.
[20] *Id.*
[21] 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.
[22] Eleni Manis et al., *Scan City: A Decade of NYPD Facial Recognition Abuse* (Surveillance Technology Oversight Project, July 8, 2018).
[23] *Inside the NYPD's Surveillance Machine*, AMNESTY INTERNATIONAL, https://banthescan.amnesty.org/decode.
[24] 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.

SURVEILLANCE
RESISTANCE
LAB

Testimony of Alli Finn on Biometric Surveillance Technologies
on Behalf of the Surveillance Resistance Lab

May 3, 2023 Hearing on the Use of Biometric Identification Systems in New York City
New York City Council Committee on Technology and Committee on Civil and Human Rights

I'm testifying today on behalf of the Surveillance Resistance Lab, an NYC non-profit organization that focuses on corporate and state surveillance systems, as one of the greatest threats to democracy, racial equity, economic justice, and migrant justice. We fight for accountability and government divestment from technologies that expand systems of control and punishment (as well as suppress dissent and difference) in public spaces, schools, workplaces, and at and across borders. Our work grows out of the Surveillance, Tech, and Immigration Policing Project, formerly housed at the Immigrant Defense Project.

Biometric surveillance technologies including facial recognition are a monumental threat to democracy and to people's rights and security, not only their privacy. Facial recognition technology can allow government, law enforcement, and private users to automatically, instantly identify people and track everywhere we go, with chilling consequences.[1]

We urgently call on the City Council to pass Int. 1014-2023 and Int. 1024-2023, to restrict use of facial recognition and other biometrics surveillance technology in multioccupancy residential buildings and in places of public accommodation (like retail stores, restaurants, entertainment venues) to verify identity. However, these bills are only one step towards full protection of our communities. We need a full ban on government and private use of biometrics surveillance technology in New York City, following the actions of other jurisdictions including Boston and San Francisco. Our current regulations, primarily Local Law 3 of 2021, which requires that certain commercial establishments post notice to customers on the collection and use of biometric identifier information, falls far short. In the absence of state and federal regulations, we urgently need the City Council to act to protect New Yorkers.

Numerous advocates and researchers have deemed facial recognition and other forms of biometrics surveillance so dangerous that its use cannot be justified. My testimony today will focus on three reasons:

1. Biometrics surveillance has been increasingly weaponized, across the world and in our city, to take away people's rights, liberties, and access to basic resources.

Over the past several years alone, facial recognition systems in the United States have been used to criminalize poverty, facilitate mass arrests and incarceration of BIPOC communities, surveil demonstrators exercising their First Amendment rights at protests, and target immigrants for deportation.[2]

The MSG Entertainment case[3] shows how easy it is for companies and law enforcement to implement invasive biometrics surveillance systems with justifications around "public safety," and then use these technologies to target people whom they designate to be "threats," advancing corporate and government

[1] https://www.newsweek.com/police-under-pressure-ban-facial-recognition-technology-1792740

[2]https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html, https://www.amnesty.org/en/latest/news/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/, https://www.fastcompany.com/90801956/in-texas-facial-recognition-is-becoming-a-way-of-life, https://americandragnet.org/.

[3] https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html

interests at the cost of people's liberties. The lawyers denied entry to sports games, Rockettes' performances, and concerts did not pose a safety concern, and yet MSG used the same system supposedly implemented for public safety to identify and remove them. Without action by the City, MSG can continue to use biometrics surveillance technology to deny entry to parents accompanying their children to the Rockettes. Business owners can continue to racially profile shoppers. Corporate landlords can continue to criminalize their rent-stabilized and low-income tenants and track their movements.

Biometric surveillance technologies do not make people safe.[4] Surveillance is not a less violent alternative to policing, it is and has been a central part of policing systems, whether deployed by law enforcement, corporate landlords, or other business entities.

2. Increased accuracy rates will not fix the fundamental flaws of biometrics surveillance technology.
Biometrics and other surveillance technologies often rely on algorithms that have been repeatedly shown to reinforce racist and other structural biases[5] and target Black, brown, poor and working class, immigrant, Arab, Muslim, and South Asian, queer and trans, and other over-policed communities.

Some of the companies that profit off facial recognition and other biometrics surveillance claim increased accuracy as a solution to unacceptable incidents of harm. But even if the technology were 100 percent accurate, its use could still result in disparate impacts, racially and beyond. Surveillance cameras and other security and policing systems are disproportionately over-deployed in Black and brown communities, by both government and private entities.[6] We have also seen disproportionate police use of surveillance technology and targeting of racial justice movements and protests in our city.[7] This exposes BIPOC, immigrant, and other targeted communities to increased use of facial recognition and reinforces violent over-policing and denial of basic rights. Surveillance cameras in private businesses are often deployed in these efforts.

3. Biometrics surveillance does not only rely on the collection of faceprints and our other data, but unregulated, mass data sharing systems that exacerbate the risks.
Biometrics-–like face prints, iris scans, DNA—are largely permanent and unique to each individual. Once someone's faceprint is collected and associated with other personally identifiable information, it creates a risk of persistent surveillance, where companies, government, and law enforcement are able to identify and track people covertly.[8] Companies that use facial recognition and vendors providing their facial recognition systems have virtually no restrictions over how they treat facial scans and all the other data they collect. As

[4] https://www.eff.org/deeplinks/2021/10/resisting-menace-face-recognition
[5] https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist, https://www.theverge.com/2020/3/3/21163013/ice-new-york-risk-assessment-algorithm-rigged-lawsuit-nyclu-jose-velesaca, https://www.theverge.com/2021/7/15/22578801/black-teen-skating-rink-inaccurate-facial-recognition.
[6] https://www.eff.org/deeplinks/2021/10/resisting-menace-face-recognition, https://www.newamerica.org/oti/briefs/civil-rights-concerns-regarding-law-enforcement-use-of-face-recognition-technology/.
[7] https://www.cnn.com/2019/01/18/us/nypd-black-lives-matter-surveillance/index.html
[8] 85 Fed. Reg. 74191 ("CBP retains biographic records for 15 years for U.S. citizens and lawful permanent residents and 75 years for non-immigrant aliens . . . Records associated with a law enforcement action are retained for 75 years . . . ."); https://www.aclu.org/news/immigrants-rights/cbps-plan-to-expand-face-surveillance-at-airports-is-a-civil-liberties-disaster-in-the-making.

far as we know, many vendors can keep data indefinitely and we have little idea who has access to it and the extent of who it is shared with or sold to.

We do know this information is often shared between corporations, law enforcement agencies, and with foreign governments. For example, Immigration and Customs Enforcement (ICE) officials have mined state driver's license databases using facial recognition technology, analyzing millions of driver photos without people's knowledge.[9] Clearview AI, a software company that significantly expands the reach of facial recognition, has built a massive facial recognition database by scraping and scanning billions of personal photos from the Internet, including social media sites—without consent.[10] Clearview AI sells and shares access to this trove of personal, private information to law enforcement agencies, private businesses, and international entities and police departments, including in New York City and in countries with anti-LGBTQ policies.[11]

Biometrics surveillance increases the power of those who hold the technologies, not the people they claim to protect. In the case of public accommodations and residential use, that means increasing the power of massive corporations like MSG Entertainment and landlords. In the case of other use of facial recognition, that often means policing agencies, which already deploy disproportionate force against Black and brown people, immigrants, Arab, Muslim, and South Asian, and queer and trans people. It also means increasing the power of those aiming to identify who seeks reproductive healthcare, who protests, who worships in specific places, and beyond.

Today, we ask the Council to do its part in protecting tenants and New Yorkers across the city. We ask you to limit the power of corporate entities to extract our data for their profit and their systems of control. Biometrics surveillance technology is not only a privacy issue. This is about housing rights. It's about economic justice. It's about racial justice. It's about true public safety. It's about what kind of city we want to be, and who the city is for.

[9] https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html.
[10] For more information, please review this FOIA request submitted by the Immigrant Defense Project, Mijente, Just Futures Law, and the American Civil Liberties Union of Northern California in 2020: https://www.immigrantdefenseproject.org/wp-content/uploads/2020/10/2020.10.19-ACLU-NC-JFL-IDP-Mijente-FOIA-re-Clearview-AI_.pdf
[11] https://www.technologyreview.com/2021/04/09/1022240/clearview-ai-nypd-emails/, https://www.markey.senate.gov/imo/media/doc/Markey%20Letter%20-%20Clearview%20II%203.3.20.pdf

TSCI

The Smart Community Initiative

Testimony before the City Council Committee on Technology - 5/3/23

Good afternoon, Members of the New York City Council on Technology, elected officials and guests, gathered here today. Thank you for giving me the opportunity to speak about technology, security and safety in New York City.

My name is Stuart Reid. I am the Co-Chairman of The Smart Community Initiative, Inc., TSCI (www.thesmartci.org), a 501c3 not-for-profit partnership of public housing resident leaders and veteran NYC-based community technologists, who have come together to help improve the quality of life for our residents utilizing innovative technology applications and services.

While TSCI certainly applauds the Council's efforts to rein in and regulate the use of technology to monitor and surveil in the name of public safety, particularly with the accelerated implementation of AI, TSCI encourages the Council to also invest its attention and resources to support successful community-based public safety initiatives utilizing innovative technology to keep our public housing developments safe.

TSCI believes that our communities themselves should be in control of our own public safety and security, rather than some third party technologists, agency or government entity. TSCI and its directors have been working in partnership with public housing resident associations for over a decade on this very issue.

TSCI trains residents in emergency and public safety communications procedures and protocols utilizing mobile radios, smart phones and other communications devices to stay in touch with each other and to keep our communities informed. Working in collaboration with resident association leadership, TSCI installs *Emergency Digital Bulletin Boards* in building lobbies that display and announce emergency preparedness and mitigation information, as well as development news and information,

TSCI also works with residents in creating the *Virtual Tenant Patrol* service, which enables residents to view live images of their building lobbies, entrances and other public spaces on mobile phones and connected devices. Where residents, many of them seniors, previously sat in building lobbies to monitor and report on suspicious traffic in their

building, they now are able to do so remotely without sitting directly in what could be harm's way.

The *Emergency Digital Bulletin Board* and *Virtual Tenant Patrol* services put public safety and quality of life directly into the hands of residents. The service is completely controlled by resident leadership, including programming of emergency and building announcements, and also serving as an information kiosk.

When everyone can see what's going on in the development, when everyone is informed and aware of their building conditions, threats and safety protocols and responses, the community itself becomes its own watchdog and first responder as we all work together to keep each other safe.

In summary, as it reviews the abuse and possible threats of biometric surveillance and AI, TSCI encourages the Council to explore community-based technological solutions to public safety that are already being successfully deployed to empower our communities to take control of and realize true public safety and security.

Thank you.

Good afternoon, my name is Hally Thornton, I'm a resident of Brooklyn, and I am testifying on behalf of Fight for the Future in support of passing legislation that prohibits the use of facial recognition technology in places of public accommodation.

Fight for the Future is a digital rights organization with over 2.5 million members nationwide, including over 85,000 in New York City.

At Fight, we believe facial recognition is more like biological weapons than it is like alcohol or tobacco. It poses such a threat to safety and the future of liberty that it cannot be effectively regulated. It must be banned.

Let's be clear, legislation that OKs the use of facial recognition in public as long as people "consent" to its use is well-meaning but misguided. Someone cannot meaningfully consent to this technology when they can't know or judge its far-reaching future harms, which could include identity theft, the sharing of data with other parties, and applications that augment bias and discrimination. It's unethical and irresponsible to put the onus on individuals to defend themselves against facial recognition or any other insidious technology with the potential for causing mass-level harm.

The city of Portland, Oregon, has taken the courageous and critical 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.

We're at a crossroads - a pivotal moment in history. If we continue to allow facial recognition use to spread among private businesses and law enforcement agencies, we're headed straight for a future in which we're tracked and watched everywhere we go, where privacy is a relic of the past, and authoritarian government control is totally pervasive. Is that the future we want? The decisions we make today about technology and the policies that govern it are going to shape not just the next 10 years, but the entire future of our communities. Because of this, I urge the council to pass the strongest possible restrictions on facial recognition. Thank you.

From: Thomas.Mannix@wakefern.com
Date: May 3, 2023 at 5:19:02 PM EDT
To: District34 <District34@council.nyc.gov>
Subject: [EXTERNAL] Biometrics

Good afternoon Council Member Gutierrez , My name is Thomas Mannix I'm a Retired New York City Police Detective . I served 26 years of service in the Transit Bureau of the NYPD . It was my privilege to server the Greatest City in the world . I was a viewer of today (5/3/23) committee meeting on Technology & Civil and Human Rights . I would like to support Jay Peltz testimony . I represent the ShopRite supermarkets on Staten Island . My brother Kevin Mannix owns the ShopRite store of Staten Island . I own the security company that keeps our stores safe . That is a major challenge these days . Facial recognition is used in our establishment . We utilize this technology the utmost diligence in reference to using this technology responsibly . We don't just say that . We are supported by our cooperative Wakefern which owns more the 300 stores along the east cost . Wakefern has safeguard in place to protect customers as well as the business cooperative. Please helps us protect our customers , associates and our community. Please help the supermarket industry . Their are enough food desserts in our wonderful city . Please support utilize of business to use the tool to keep our stores, customers and associates safe . Even though you don't represent my district , I know from the committee meeting today , you represent our city fairly . Please help us . Stay safe Thomas Mannix

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: 05/03/23

(PLEASE PRINT)

Name: Francisco Marte

Address: _____

I represent: Bodegas & Small Business

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1014, 1024 Res. No. _____

☑ in favor ☐ in opposition

Date: 5/3/23

(PLEASE PRINT)

Name: Alli Finn

Address: 312 E 7th St, Brooklyn NY 11218

I represent: Surveillance Resistance Lab

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1014 1024 Res. No. _____

☑ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: DANIEL SCHWARZ

Address: 125 BROAD ST

I represent: NEW YORK CIVIL LIBERTIES UNION (NYCLU)

Address: 125 BROAD ST

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

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1014 Res. No. 1024

☐ in favor ☒ in opposition

Date: 5/3/2023

(PLEASE PRINT)

Name: ROBERT TAPPAN

Address: 1325 G STREET, NW #500, WASHINGTON, DC

I represent: INTERNATIONAL BIOMETRICS + IDENTITY ASSN

Address: SAME AS ABOVE

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 3300 Res. No. 3301

☐ in favor ☐ in opposition

Date: 5/3/23

(PLEASE PRINT)

Name: Hallie Thornton

Address: [redacted] 22nd St [redacted] Brooklyn, NY 11215

I represent: Fight for the Future

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: Michael Pitcherstack

Address: Chief Privacy Officer

I represent: City of New York Technology & Innovation

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: Fitzpatrick Office

(PLEASE PRINT)

Name: Ryan Birchmeier, York

Address: Deputy Commissioner

I represent: NYC Office of Technology

Address: & Innovation

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: Albert Fox Cahn

Address: _____

I represent: Surveillance Tech. Oversight Proj.

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: Hillary Scrivani

Address: _____

I represent: NYCCHR (Senior Policy Counsel)

Address: 22 Reade St, fl. 2

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. 1014 Res. No. _____

☐ in favor ☑ in opposition

Date: 5/3/23

(PLEASE PRINT)

Name: Jay Peltz

Address: _____

I represent: Food + Justice Alliance of NY

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. 1014 1024 Res. No. _____

☐ in favor ☑ in opposition

Date: 5/3/23

(PLEASE PRINT)

Name: JAKE Parker

Address: 8455 Colesville Road, Silver Spring MD

I represent: Security Industry Association

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: May 3, 2023

(PLEASE PRINT)

Name: Stuart Reid

Address: New York, NY

I represent: The Smart Community Initiative

Address: 1039A Lafayette Ave, Bklyn NY

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. 1014 + 1024 Res. No. _____

☒ in favor ☐ in opposition

Date: 5-3-2023

(PLEASE PRINT)

Name: Lisa Meehan

Address: _____

I represent: Mobilization for Justice

Address: 100 William St. New York NY 10038

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