CITY COUNCIL
CITY OF NEW YORK

---------- X

TRANSCRIPT OF THE MINUTES

Of the

COMMITTEE ON CONSUMER AND WORKER PROTECTION

---------- X

Friday, February 24, 2023
Start: 10:25 a.m.
Recess: 12:36 p.m.

HELD AT: 250 Broadway Committee Room
14th Floor

B E F O R E: Marjorie Velázquez, Chairperson

COUNCIL MEMBERS:
Shaun Abreu
Gale A. Brewer
Amanda Farias
Julie Menin
Chi A. Ossé
Julie Won

A P P E A R A N C E S (CONTINUED)

Jumaane Williams
Public Advocate
City of New York

Carlos Ortiz
Assistant Commissioner
External Affairs and Policy
New York City Department of
Consumer and Worker Protection

Brad Hoylman-Sigal
Senator, 47th District
New York State Senate
(speaking also for:
Tony Simone
Assemblyman District 75
New York State Assembly)

Samuel Davis, Esq.
Senior Partner
Davis, Saperstein & Salomon

Meg Foster
Legal Fellow
Center on Privacy and Technology
Georgetown Law

Nina Loshkajian
Legal Fellow
Surveillance Technology Oversight Project

Jake Parker
Senior Director, Government Relations
Security Industry Association

Jeramie Scott
Senior Counsel
Electronic Privacy Information Center

Andrew Rigie
Executive Director
New York City Hospitality Alliance

Daniel Schwarz
New York Civil Liberties Union

Leila Nashashibi
Fight For The Future

Alli Finn
Senior Researcher and Organizer
Surveillance Resistance Lab

Jason Berger
Coalition for Ticket Fairness

Tom Ferrugia
Director of Governmental Affairs
The Broadway League

James Sullivan
Senior VP of Strategy and Compliance
Chief Legal Officer
BIO-key

Attiya Latif
Staff Organizer
New York Ban The Scan Task Force
Amnesty International USA

SERGEANT AT ARMS: Good morning and welcome to the Committee on Consumer and Worker Protection. At this time we ask if you could please place phones on vibrate or silent mode. Thank you for your cooperation. Chair, we are ready to begin.

CHAIRPERSON VELÁZQUEZ: Good morning. My name is Marjorie Velázquez and I am the Chair of the Committee on Consumer and Worker Protection. And welcome to our committee hearing on the use of facial recognition technology in New York City businesses, and the proposed Intro No. 8-A related to the disclosure of total ticket costs and advertisements for entertainment events in New York City.

I'd like to acknowledge my colleagues here on the committee. I have Councilmember Shawn Abreu. I have Councilwoman Julie Won. I have Councilmembers Chi Ossé, who are on Zoom. And I have public advocate Jumaane Williams.

So New York City is one of the world's pre-eminent centers for live entertainment and events. We are the home of Broadway, iconic sport franchises, Yankees (got to give them love, sorry, Mets), and renowned venues large and small.

As the Chair of Consumer and Worker Protection Committee, it is of the utmost importance that me and that New Yorkers receive honest, transparent, and fair treatment from event venues and other commercial establishments. All too often, however, when consumers go online to buy tickets to events, they are surprised by fees that increase the cost by as much as 20%. The bill that we are hearing today, which is sponsored by Councilmember Brennan, would help address the surprise costs by requiring event operators and ticket sellers to include the entire cost of the ticket, including taxes and fees, especially in their advertisements. This disclosure would help consumers understand the full cost of a ticket price upfront, rather than being surprised later.

The other topic we are here to address is the use of facial recognition technology in New York City businesses.

Once the realm of science fiction, technological advances in recent years have made facial recognition technology affordable and effective for a wide range of commercial uses. While facial recognition technology has the potential to be used in a positive

way that would help improve safety and efficiency in businesses, it also poses new consumer protection challenges.

In response to the growing use of this technology and concerns about New Yorkers privacy and consent, in 2021, the council passed legislation that requires New York City businesses to inform customers if facial recognition technology is in use, and it also prohibits businesses from selling any facial recognition data that they collect.

Despite significant improvements in recent years, facial recognition remains an imperfect technology that misidentifies people of color, women, and young people. Even very small error rates can impact large numbers of other members of people in the city as large as ours, and misidentification can have significant consequences on those affected.

Facial recognition relies on large stores of valuable personal data, making the systems a potential target of security breaches, information leaks by careless or corrupt employees, or even foreign intelligence agency break ins. Companies that develop facial recognition software sometimes use deceptive tactics to expand their databases or

improve their products, and as more entities gain access to facial recognition technology it increases the potential for improper use.

Like many people, I am extremely concerned about the reports that MSG is using facial recognition to enforce a ban on lawyers who work at firms involved in litigation with the company. According to the New York State Attorney General, as many as 90 firms and thousands of lawyers are affected by this ban, regardless of whether the attorneys have any relationship to the litigation against the company.

As a result of the policy multiple ticket holding patrons have been denied entry to sporting events, concerts, and performances at Madison Square Garden owned properties.

One of the people impacted was attorney Kelly Conlon, who was denied entry to the Radio City Music Hall was chaperoning her daughter's Girl Scout troop to a Rockettes show.

Facial recognition identified Ms. Conlon as she went through the metal detectors, and security guards forced her to wait outside while her daughter and the other members of the Girl Scout troop and their mothers got to enjoy the performance.

Ms. Conlon's law firm is involved with a personal injury case against a venue owned by Madison Square Garden, but she has nothing to do with the case and doesn't even practice law in New York.

While we certainly do not want to stand in the way of technological advancements, we must do what we can as a city to protect New Yorkers' privacy and information and ensure that these products are not used in ways that harm consumers and workers.

We are here today to learn more about how New York City businesses are employing facial recognition technology, as well as the benefits and risks associated with its use. I look forward to hearing from a range of witnesses on both of these important consumer protection topics, and I'll now turn it over to Public Advocate Jumaane Williams to make his statement.

PUBLIC ADVOCATE WILLIAMS: Thank you so much, Madam Chair. As was mentioned, my name is Jumaane Williams, Public Advocate for the City of New York. I want to thank CHAIRPERSON VELÁZQUEZ and the members of the Committee on Consumer and Worker Protection for holding this hearing up allow me to say a few

words. I just want to align myself with your words and your awesome article in our city and state today.

Fundamentally, New Yorkers are protected by the First Amendment right to privacy. Individuals should expect that they can freely conduct private transactions without being surveilled. To that end in 2021, my office partner with then Borough President Gale Brewer, Amnesty International, STOP and AI For The People on the Ban The Scan Campaign, raising awareness of the dangers of public and private use of facial recognition AI.

At that time, I asked the previous administration to cease use of all facial recognition technology, permanently destroy data collected and used for facial recognition in the past, and published data concerning each instance in which facial recognition technology was utilized.

Through non-consensual data capture, businesses violate the right to privacy, and we've also seen much concern when it comes to law enforcement. Individuals should not be removed from a place of business because their employer is involved in legal action against said business, especially when the business engages in its trade in the case at hand

selling tickets to events, and then reneges to allow the purchaser employee to redeem the ticket they purchased. The employee is not involved in litigation.

If any business could monitor and remove people because of a grievance against an employer or someone they have a relationship with, it would mean a world where businesses have the right to bar anyone from any establishment based on a tangential connection. Moreover, there was another instance where a parent was denied entry to an event on a school trip in which they were serving as an escort. This act create a safety risk for the children as well as creating a stressful situation for the other adults who had to care for more children on their own.

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

While there are security concerns that impact the decision making of private businesses and City of New York cannot let businesses broadly use facial recognition technology and run afoul of everyone's right to privacy has granted under the US Constitution.

It is important to note that many documented instances of facial recognition technology have racial and gender biases. Researchers at MIT reported in January 2019 that facial recognition software marketed by Amazon misidentified darker skinned women 31% of the time, while others have shown that algorithms used facial recognition return false at a higher rate for African Americans than white people unless explicitly recalibrated for a black population.

Specifically technology misidentified people talk complexions 15% of the time, as compared to only 3% of time with light complexions. We also know and have heard similar numbers when it comes to people of the transgender experience. These findings prompted experts at Google, Facebook, and Microsoft to sign a letter calling on Amazon to stop selling its facial recognition technology to law enforcement.

Also, facial recognition technology is only one of several biometric technologies being developed for identification purposes. Others include long-range cardiac signature detection, gait analysis, and an iris scan. We must engage discussions on how to address and prevent the use and abuse of all these technologies. It can't be left up to businesses and big corporations or a few billionaires and millionaires.

I also just want to say as a person who suffers from the disease of Knick fandom, when it comes to MSG I have been scarred by many decisions of the owner, James Dolan. (I have to say it's getting a little better now, so I will put that out there.) But as a New Yorker, many of the antics of the owner are much worse, much more harmful: from removing people from MSG, to this now use of facial recognition. I do want to put on the record that I also believe we should be reviewing the renewal of the tax abatements and exploring moving MSG as well. My hope is that someone would have been here for MSG to answer some of these questions. It is really important. All-- there's a point where private and public really come in connection, and we can't allow

just run amok, and government has to step in. So I'm glad we're having this hearing. Thank you very much, Madam Chair.

COUNSEL SWAIN: Thank you CHAIRPERSON VELÁZQUEZ and Public Advocate Williams. Good morning and welcome. My name is Sarah Swain, Counsel to the Committee on Consumer and Worker Protection, and I will be moderating this hearing.

Before we begin, I'd like to remind everyone who is joining us via Zoom that you will be on mute until you are called on to testify at which point you will be asked to accept to be unmuted by the host. I'll be calling on public witnesses to testify after the conclusion of the Administration's testimony and Councilmember questions, so please listen carefully for your name to be called.

At this hearing, we will first be inviting testimony from the Department of Consumer and Worker Protection, followed by testimony from members of the public. Councilmembers, you will be called on for questions after the panel has completed their testimony. Please note that Councilmembers will have three minutes for questions, and we will be allowing a second round of questioning if needed.

We will now call on representatives of the Administration to testify. We will be hearing testimony from Carlos Ortiz, Assistant Commissioner of External Affairs and Policy at the Department of Consumer and Worker Protection.

At this time I will administer the affirmation.

Please raise your right hand.

Do you affirm to tell the truth, the whole truth and nothing but the truth before this committee and to respond honestly to Councilmember questions?

ASSISTANT COMMISSIONER ORTIZ: I do.

COUNSEL SWAIN: You main begin.

ASSISTANT COMMISSIONER ORTIZ: Good morning, CHAIRPERSON VELÁZQUEZ, Public Advocate Williams, and members of the Committee on Consumer and Worker Protection. My name is Carlos Ortiz, and I'm the Assistant Commissioner for External Affairs at the Department of Consumer and Worker Protection. Thank you for the opportunity today to testify on Introduction 8-A relating to the disclosure of service free charges for tickets to entertainment events in New York City.

When it comes to price transparency, DCWP is committed to leading efforts to protect New Yorkers.

One of the main ways that DCWP does that is by enforcing the Consumer Protection Law, which prohibits illegal trade practices, like deceptive advertising, that prey on consumers. DCWP also enforces protections governing disclosures of refund policies, layaway plans, and the sale of secondhand items. Businesses may at times hide costs to consumers by tacking on a variety of fees, such as service or processing fees, to an initial product price. The consumer may only find out the true cost of an item at the end of the at the end of a transaction. This drip pricing approach is frustrating for consumers, and can make it harder for them to budget for their purchases.

Over the years, DCWP has supported regulatory initiatives to promote price transparency and reduce junk fees on the state and federal levels. In 2022, New York State passed a law that requires operators, ticket platforms, and ticket resellers to disclose the total cost of a ticket prior to the ticket being selected for purchase. The Consumer Financial Protection Bureau also launched a federal initiative to reduce or eliminate junk fees, such as overdraft

or non-sufficient fund fees, which cost Americans billions of dollars annually.

Likewise, other federal agencies, such as the Federal Trade Commission and the Department of Transportation have recently pursued rule changes to crack down on junk fees and increase price disclosures. DCWP has submitted comments in support of these and other similar efforts to ensure price transparency at the local level.

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

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

Thank you again for the opportunity to testify today about the disclosure of service fee charges for entertainment tickets, a problem that many New Yorkers know all too well.

I look forward to any questions you may have. Thank you.

CHAIRPERSON VELÁZQUEZ: Thank you, Carlos. So does DCWP know how many commercial businesses in New York City use facial recognition technology?

ASSISTANT COMMISSIONER ORTIZ: Thank you Chair. No. That is not information that we that we have at DCWP. Although -- I'm sorry -- I would mention, pursuant to your opening statement, commercial businesses are required to post signage if they are collecting biometric data such as facial recognition, retina scans, fingerprints, et cetera.

CHAIRPERSON VELÁZQUEZ: And has DCWP ever received any consumer complaints related to the use of facial recognition technology by commercial businesses or...?

ASSISTANT COMMISSIONER ORTIZ: Apologies. No. We have not received complaints with respect to the collection of biometric data. In that particular case of that local law that is enforced by a private

right of action. So a New Yorker is able to bring that case forward on their own, should there should there be a violation that's observed.

CHAIRPERSON VELÁZQUEZ: So if someone just calls 311 to complain, you just tell them, "Hey, resolve this privately"? I'm not sure of the-- the exact-- what exactly is said. But I think they will be advised that there's-- that they have a right-- a private right of action with respect to this local law.

CHAIRPERSON VELÁZQUEZ: So if someone is misidentified in a commercial context, what is their recourse?

ASSISTANT COMMISSIONER ORTIZ: What do you mean by misidentified?

CHAIRPERSON VELÁZQUEZ: So let's use the example of going into Madison Square Garden for a concert, Bad Bunny, and-- and all of a sudden, it misidentifies me as someone that they do not want there, and I am removed. What is my recourse?

ASSISTANT COMMISSIONER ORTIZ: Well, I think certainly when a consumer-- whenever you're purchasing a good or service, for example, a ticket, there are of course terms and conditions that are

agreed upon, that would outline for example, what refund policy might exist, and what-- what recourse that the consumer might have.

I'd also say that if a consumer does feel that they've been targeted by a deceptive action, that they can always file a complaint with the Department of Consumer and Worker Protection, and we'll look into the facts of the complaint and see if there's something we can mediate, if it's something we can investigate on behalf of the consumer, or multiple consumers if that's the case.

CHAIRPERSON VELÁZQUEZ: So they'd be calling you directly, instead of 311, you think?

ASSISTANT COMMISSIONER ORTIZ: I mean, certainly, I'm always-- my team is always available be called directly. And I know I've mentioned the past, but you can contact us at Community Affairs at DCWP.nyc.gov. 311, of course, is also an option, as well as our website does have functionality to submit complaints.

CHAIRPERSON VELÁZQUEZ: And then after I go ahead and call you guys, do you start an investigation? And what kind of support would you be able to provide the consumer that has been...?

ASSISTANT COMMISSIONER ORTIZ: Generally when I when I've had to deal with this in the past, I would ask the consumer for any type of documentation relating to their complaints, and that would I think, help us start establishing any relevant facts. I think from there, it's really a case-by-case basis on what-- what those documents point to, the particular allegations or observations that took place with respect to a complaint.

CHAIRPERSON VELÁZQUEZ: Does DCWP have any concerns about the use of facial recognition technology by commercial businesses?

ASSISTANT COMMISSIONER ORTIZ: I think-- I mean, personally, I think I recognize that it's a significant issue for many New Yorkers. And I can see, particularly, if the council is having a hearing on it as well.

From the perspective of the department, I do feel that we-- we don't necessarily have the expertise around facial recognition technology or its implementation to provide a particular position.

CHAIRPERSON VELÁZQUEZ: So I guess, like in our hearings next month for funding, maybe we can have a conversation on that.

ASSISTANT COMMISSIONER ORTIZ: Well, I would--

CHAIRPERSON VELÁZQUEZ: Funding the Agency to have more inspectors and whatnot.

ASSISTANT COMMISSIONER ORTIZ: I don't-- I don't think I would ever-- I wouldn't be doing my job if I didn't say that I thought resources were important for our agency. Um, I do consider consumer and worker rights in New York City to be one of the most important things we can be working on. That said, I know our-- our commissioner has been focused on-- on making sure that our agency stays centered on our mission, whether it's deceptive trade practices, whether it's workplace rights.

And I with this administration as well, that there's been a concerted effort to build ties between different agencies to tackle multidisciplinary issues, such as this perhaps.

CHAIRPERSON VELÁZQUEZ: All right. Thank you. Councilmember Brewer? Public Advocate? Okay.

COUNCILMEMBER ABREU: Thank you. My question is: Does DCWP have any concerns about the use of facial technology, facial recognition technology?

ASSISTANT COMMISSIONER ORTIZ: Thank you, Councilmember. I think, um, I would really have to

defer to perhaps other subject matter experts around facial recognition technology. This is not something that we have enforcement authority over necessarily.

I think the-- the core of our work as it relates to consumer protection is really about preventing deception or other similar type practices. That isn't to say that consumers can be adversely affected by certain business practices outside of that. But that's where I think I might rely on-- on another-- another agency with closer ties to that.

COUNCILMEMBER ABREU: Does the DCWP have concerns about the storage of biometric data by consumer businesses?

ASSISTANT COMMISSIONER ORTIZ: Again, I think I'd have to defer again on that question, Councilmember. I'm sorry.

You know, our understanding was that um, we will be discussing primarily Introduction 8 and it's-- and it's overlay with price transparency, which really falls into kind of the bailiwick, so to speak, of our agency.

In terms of facial recognition technology, that's not something that-- that we currently are involved

in, or have a have a level of technical expertise for.

COUNCILMEMBER ABREU: If we were to assume that there was storage of biometric data consumer businesses, that would not be a concern to the Administration?

ASSISTANT COMMISSIONER ORTIZ: No. I wouldn't say that, sir. I would say--

COUNCILMEMBER ABREU: So there would be a concern?

ASSISTANT COMMISSIONER ORTIZ: I don't want to speak for other agencies. What I meant to say by my answer: I'm saying from the perspective of DCWP, it's not something that we work on, or that we have the expertise for.

COUNCILMEMBER ABREU: All right, thank you. What is the Administration's position on limiting the use of facial recognition-- recognition technology in New York City businesses? I'm assuming it's probably the same?

ASSISTANT COMMISSIONER ORTIZ: Yes, sir. I think it's the same answer there. I know, in the past, the council and the previous administration did work on a particular local law around biometric data. But

again, I think that the touch point for our agency there was-- was much more in line with what we do in our consumer protection work, which is signage requirements. But we don't have any particular enforcement authority over that. If-- if you would be interested in more information for the Administration, I'm happy to connect with the Mayor's Office of City Legislative Affairs, and I think they could probably answer more questions specifically on the Administration's position of facial recognition.

COUNCILMEMBER ABREU: Yeah, I would definitely like answers to those questions.

Does the Administration support Assembly Bill, A-1362, which would establish a statewide Biometric Privacy Act?

ASSISTANT COMMISSIONER ORTIZ: I'm not familiar with that legislation myself. I think I'd have to take a-- read a bit first, before I could provide a position on it.

COUNCILMEMBER ABREU: And last question I have is: Does the Administration support federal legislation that would limit the ways in which the private sector may collect and use biometric data?

ASSISTANT COMMISSIONER ORTIZ: I think likewise there, I mean, with any with any type of legislation, we're happy to take a look at it and figure out what-- what is-- what value it could be bringing to New Yorkers, how we protecting them from all types of business activities, or whether that's discrimination, or whether that's violations of privacy, such as the Public Advocate meant? I think the Administration is always interested in looking into that.

But for those cases, since they fall out of kind of the bailiwick of our agency, I would refer you to-- to the Mayor's Office for further comment on that.

COUNCILMEMBER ABREU: Thank you. And my final question is: Does DCWP have any concerns about enforcing Proposed Intro 8-A?

ASSISTANT COMMISSIONER ORTIZ: No, not necessarily. I think we feel like this is like the core of our work. We think it's an important protection. Price transparency is something that we want to ensure for all consumers in New York City.

We do have suggestions of how to expand its scope somewhat to-- to make sure that consumers from the point of they're looking into a ticket to the point

of actually buying the ticket have all the information in front of them. So we're happy to work with counsel on that, as we get through the legislative process.

COUNCILMEMBER ABREU: I appreciate your openness there. Thank you.

ASSISTANT COMMISSIONER ORTIZ: Yeah, of course.

PUBLIC ADVOCATE WILLIAMS: Thank you. You mentioned -- I think it was either testimony or under questioning -- that the businesses have to post whether they're using facial recognition.

ASSISTANT COMMISSIONER ORTIZ: That's correct, sir.

PUBLIC ADVOCATE WILLIAMS: Are you aware if MSG has a posting?

ASSISTANT COMMISSIONER ORTIZ: I'm not aware if they have a posting, myself.

PUBLIC ADVOCATE WILLIAMS: Are you aware of any other rules or regulations as related to facial recognition?

ASSISTANT COMMISSIONER ORTIZ: No. I'm most familiar with this local on biometric data signage, because it's something that the past administration worked on with the Council and with our agency.

PUBLIC ADVOCATE WILLIAMS: So is it-- I know you said you-- you're not an expert. But is it fair to assume that there's not much more rules and regulations around picture recognition?

ASSISTANT COMMISSIONER ORTIZ: I don't-- I mean, the City-- the city agencies is a wide landscape. I-- I don't want to assume too much with respect to what other protections might be in place. I know-- I know that there are of course protections with respect to discrimination, both at the city and state level. I know that there-- that if any crimes are committed, there's certain protections there as well, I think-- I wouldn't want to assume necessarily what is in place right now outside of my agency.

PUBLIC ADVOCATE WILLIAMS: Got it. I would presume -- hopefully, I'm wrong, but I don't think so -- that there is a lot more regulations and policies that need to be put in place, which is-- which is part of the problem.

ASSISTANT COMMISSIONER ORTIZ: Yes.

PUBLIC ADVOCATE WILLIAMS: And also, if I understand correctly, the recourse, the only recourse that someone has now, if they feel like their rights

are violated for the use of facial recognition, is a private right of action.

ASSISTANT COMMISSIONER ORTIZ: Yes. That particular law requires that any business that's collecting information disclose it via signage, and the only-- the only recourse in that sense is-- is a consumer-- a consumer's private right of action, sir.

PUBLIC ADVOCATE WILLIAMS: Thank you. I also just wanted to mention, because my understanding is that MSG was invited. I don't know if I'm seeing anyone here. Hopefully, someone may come later.

If they don't come, I just want to say that I think is pretty cowardly and disrespectful to the process and to this Council. And I don't think this is the kind of thing that should only be litigated in the public.

If you believe that you should be using this you should come here and have a conversation about why, so that people can publicly understand what's happening. So I just want to make sure I put that on the record, and it's a shame that someone is not here.

But I you know-- too, if they're listening, I welcome having a conversation. I'm sure colleagues

would as well. And this is something that is too important to just try litigate it through newspapers, and media. Thank you.

CHAIRPERSON VELÁZQUEZ: Thank you so much for that, Public Advocate. I have a couple of questions on behalf of Councilmember Chi Ossé, who is with us virtually.

The first question I have is: Is DCWP doing any outreach on privacy, know your rights, to the public, or at least informing the public on what to do when they see this technology at a business? Many times an average layperson who's going to a store, an event at an arena -- MSG has been notorious and using this technology -- will not will not know what to do when they're asked to do scans, nor are they aware of any rights protections, or what happens to-- with those scans after.

So what's the public information campaign, is essentially what Chi is asking.

ASSISTANT COMMISSIONER ORTIZ: Thank you. Um, in terms of the signage that the local law requires, that is available on our website, but we don't have-- we have not-- In terms of dedicated outreach around

this, I don't think there's any-- anything that's been put in place.

CHAIRPERSON VELÁZQUEZ: Is there a reason why? Lack of funding? Lack of initiative? What is it?

ASSISTANT COMMISSIONER ORTIZ: No, I would say in terms of-- in terms of our protections, what we try to focus on is-- is outreach in things that we enforce. I think we're concerned at times of-- I think we would have a concern of, for example, doing outreach of something we don't enforce, because that would lead a consumer or New Yorker down the wrong path in terms of who they should be going to.

And in terms of that particular local law, I think our focus is on making sure that-- that the information was publicly available for people to go to if they were interested in finding out more about that. But our-- our particular outreach efforts are more focused towards consumer protection law, paid safe and sick leave, these other laws that we are actively enforcing out there and generating complaints for.

CHAIRPERSON VELÁZQUEZ: What kind of enforcement would you see DCWP being able to perform, if given the right legislation?

ASSISTANT COMMISSIONER ORTIZ: Do you mean with respect to facial recognition?

CHAIRPERSON VELÁZQUEZ: Enforcement. Yup.

ASSISTANT COMMISSIONER ORTIZ: Oh, yeah. I think it's-- it's, um, you know, it's an interesting question. I mean, generally, when you-- when you have new mandates that are being set up, there all types of resources that might be required, whether that's intake personnel, investigators. You need attorneys, of course, to be able to bring cases to oath on behalf of consumers.

I think generally, for any type of mandate, that's-- that-- those are the type of needs that we would always look at.

But again, I think we also want to build into what the mission is of the Agency. And from our perspective, you know, the mission on consumer protection is-- is around deception, you know, certain licensed-- certain licensed entities that we have.

I think, in this case of biometric data or facial recognition, it's as much a civil rights issue as it could be a consumer issue. Notwithstanding, I do think it's a consumer issue; just perhaps not one

that is-- is best tackled necessarily with DCWP as the tool.

CHAIRPERSON VELÁZQUEZ: Gotcha. The other question from Councilmember Ossé is: What is DCWP and the City as a whole doing to prevent businesses from using this data to (A) breach people's privacy, and then (B) the use of this as surveillance information to aid in getting people arrested or entangled with the carceral system?

ASSISTANT COMMISSIONER ORTIZ: Yes. So I think, probably, to take that first part of that question: Um, I don't-- I don't know if there's any anything that prevents companies from-- from collecting this data? I think the-- the one local law that I'm familiar with just requires commercial businesses to disclose that they're collecting this information.

But again, I probably would circle back with my colleagues, the Mayor's Office, or other agencies in case theres things that I'm not aware of.

CHAIRPERSON VELÁZQUEZ: Got it. All right. Now, Councilmember Menin.

COUNCILMEMBER MENIN: Oh, great. Thank you so much, CHAIRPERSON VELÁZQUEZ. Um, just a couple of questions on the biometric technology law: How many

inspectors are dedicated to enforcing this law at DCWP?

ASSISTANT COMMISSIONER ORTIZ: So the-- the law is actually enforced only by a private right of action. It is not-- It does not have administrative enforcement within it.

COUNCILMEMBER MENIN: But is it DCWP's belief that the law should be amended so that we can actually have some more teeth in this law?

ASSISTANT COMMISSIONER ORTIZ: I think-- I think from our perspective, we would-- we would have concerns if we were tasked with any type of enforcement around facial recognition technology. We just don't feel that we're the best equipped agency, necessarily, for that.

But I think, um, you know, generally, I know this administration has an openness with counsel about amendments or legislation. But again, I feel like we would probably not be the ones that would want to take up that mantle necessarily.

COUNCILMEMBER MENIN: Given though that the facial recognition technology is absolutely affecting consumers' privacy rights, has the Agency spoken to other cities about what they're doing on facial

recognition technology? Because obviously, New York is not the only city to be grappling with this. We should be looking at other cities as models, so we can figure out how to truly tackle this issue and protect consumers privacy.

ASSISTANT COMMISSIONER ORTIZ: No. I think-- I think that's a point very well taken. I think that New York City, despite being the largest and greatest city in the United States, it still can learn things from across the country. I think it's a point well-taken that it's something that the Administration can do, but the Agency itself has not had conversations around that, given our-- our lack of touchpoint with facial recognition technology and biometric data.

COUNCILMEMBER MENIN: Okay. Okay. Thank you.

CHAIRPERSON VELÁZQUEZ: Public Advocate?

PUBLIC ADVOCATE WILLIAMS: Thank you, Madam Chair for being so courteous.

I have-- I just want to understand the process. Is DCWP primarily complaint driven? Or do you go out and do investigations on your own without complaints?

ASSISTANT COMMISSIONER ORTIZ: I think it would really depend on-- on the category that we're looking at. You know, certain-- certain activity that we

might focus on, complaints for example -- Have refund policies been posted? Has certain signage been put up? -- Other types of protections we have in place might-- might be proactive investigations, such as workplace investigations of paid safe and sick leave. It really would depend, sir.

PUBLIC ADVOCATE WILLIAMS: So, since-- this is such-- the gravity of MSG, and what they're doing is so much-- can someone go out today to look and see if they have signage posted, as legally required?

ASSISTANT COMMISSIONER ORTIZ: To see-- which-- which signage? The signage from the biometric data law?

PUBLIC ADVOCATE WILLIAMS: Yes.

ASSISTANT COMMISSIONER ORTIZ: I don't know that that's something that we would do.

PUBLIC ADVOCATE WILLIAMS: I'm making a request. Officially. Is there some other way I should make it?

ASSISTANT COMMISSIONER ORTIZ: I don't know. I think-- I can certainly-- After this hearing, I can certainly circle up with our folks at-- at the Agency down-- down the street and see what we can-- what can be done there.

PUBLIC ADVOCATE WILLIAMS: Thank you.

ASSISTANT COMMISSIONER ORTIZ: And get back to you as well, of course.

PUBLIC ADVOCATE WILLIAMS: Thank you, and I'll circle around too.

ASSISTANT COMMISSIONER ORTIZ: Okay. Thank you.

CHAIRPERSON VELÁZQUEZ: Wait. Just to be clear on the request: It's all of the Madison Square Garden entertainment properties? Just to make sure.

ASSISTANT COMMISSIONER ORTIZ: Well, I-- again, I think it's something-- that's something that I'll bring back. I can't make any promises. I don't over-promise, but it's something that I will discuss with our folks, and I can get back to you today about what we can land on.

PUBLIC ADVOCATE WILLIAMS: Thank you. And if we can't, I would like to know why we're unable to.

ASSISTANT COMMISSIONER ORTIZ: Okay.

PUBLIC ADVOCATE WILLIAMS: Thank you.

ASSISTANT COMMISSIONER ORTIZ: Thanks.

CHAIRPERSON VELÁZQUEZ: Thank you so much for coming.

ASSISTANT COMMISSIONER ORTIZ: Okay. Thank you.

COUNSEL SWAIN: Thank you. And thank you Chair. We will now turn to public testimony. If you are in person, you will please come up and take a seat at the table, and you may begin once the sergeant has notified you that time has started.

You will have five minutes to testify, so please begin once the time starts. Councilmembers who have questions for a particular panelist should let me know, and I will call on you after the panelist has completed their testimony.

For panelists on Zoom, once your name is called a member of our staff will unmute you, and the sergeant at arms will give you the go ahead to begin.

Please wait for the sergeant to announce that you may begin before delivering your testimony. For those testifying in person, make sure that you press the button on the microphone and the red light goes on so that we can hear your testimony.

Our first panel will be a Zoom panel. We'll be hearing from State Senator Brad Hoylman-Sigal.

SENATOR HOYLMAN-SIGAL: Good morning. Good morning. Good morning, Madam Chair and colleagues, and the City Council Public Advocate. I'm State Senator Brad Hoylman-Sigal. I represent the 47th

Senate District, which runs from Christopher Street to 103rd on the West Side.

I'm testifying on behalf of myself and also Assemblymember Tony Simone who represents the 75th Assembly District, which covers Chelsea, Hell's Kitchen, and East Midtown, as well as part of the Upper West Side.

We're deeply concerned about the growing use of facial recognition software in public spaces by private entities. In the state Senate I carry multiple bills regulating the use of facial recognition technology, which has been a vacuum for regulation and oversight by various levels of government. So I'm very grateful to the City Council for considering this important issue.

Facial recognition technology, as I'm sure you know, has proven to be inaccurate, and discriminatory, and can lead to the misuse of personal biometric data without consent. There was a 2019 analysis by the National Institute of Standards and Technology of 189 facial recognition algorithms, the majority of the industry, and it found that this technology erroneously identifies Black and Asian faces 10 to 100 times more often than it does White

faces. The report discovered that women, the elderly, and children were also more likely to be falsely identified. And these discriminatory failures overlap. Women of color, and particularly young black women have some of the poorest identification accuracy rates of any demographic. Other research has found that these algorithms also misidentified transgender men as women 38% of the time, and non-binary people 100% of the time.

The technology also poses grave privacy concerns as has been noted, as individuals face information is usually collected without their consent, cannot be encrypted, and is therefore vulnerable to data security breaches or being resold.

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

For example, members of this committee know that recent controversy around Madison Square Garden, and Madison Square Gardens Entertainment's disturbing use of facial recognition software to identify and eject patrons from entertainment venues whom they deemed to be hostile to their legal or financial interests.

MSG Entertainment has repeatedly deployed this technology against attorneys who represent clients suing MSG, and even against people working at the same firms who have nothing to do with those cases.

This practice is deeply worrisome because it sets a precedent for private companies to chill free speech by denying access to those who disagree. This policy also violates the privacy of entertainment patrons who have no idea their biometric information is being collected at a casual sports outing.

Essentially, when you walk into Madison Square Garden, you are immediately treated as a suspect. This policy is clearly not about public safety on Madison Square Garden's part. It's about retaliation against Madison Square Garden's perceived enemies, chilling speech and access to the courts. Where does it end? Journalists? Labor? Banning someone from going to their local grocery store? The owner of Madison Square Garden Entertainment says the garden can do whatever it wants, because it's, quote, "private property." And that MSG, quote, "has a right to defend itself."

To that I would say: If it's your private property, perhaps they should be paying property taxes. That's another point.

But facial recognition technology allows Madison Square Garden to retaliate and potentially discriminate at a scale that would not be possible without the technology. This flawed technology and the manner in which it is deployed is an attack on all of our privacy and civil liberties. I carry legislation in Albany to address this issue by closing a loophole that allows the owners of Madison Square Garden to deny entry to those individuals who are attending a sporting event. It's already illegal to deny admission to Broadway musicals, public talks, and concerts if you have a valid ticket. But this loophole in New York statute is exempt sporting events from the rule and our bill would close this loophole.

Again, I want to thank the committee for investigating this use of facial recognition technology by private businesses, and I would urge you to also investigate and highlight similarly problematic uses, which we are also hoping to address in Albany, such as the use of facial recognition

technology by law enforcement and residential landlords.

Again, thank you for the opportunity to speak today. I'm hopeful we can make progress on this important issue.

CHAIRPERSON VELÁZQUEZ: Right on time. That was excellent senator.

SENATOR HOLMAN-SIGAL: Thank you. I practice.

CHAIRPERSON VELÁZQUEZ: I'd like to recognize Councilmember Farias and Councilmember Menin, who have joined us.

We wanted to thank you so much for your testimony. We are looking forward to working with you on legislation to rectify and to help impacted consumers by this.

COUNSEL SWAIN: Thank you. The next panel will be in person. It will be Samuel Davis, followed by Meg Foster, followed by Nina Loshkajian, followed by Jake Parker.

The first two panelists may take a seat at the table. Make sure that when you begin your microphone is turned on.

MR. DAVIS: Thank you Chair Velázquez and Councilmembers for inviting me to speak today at this

incredibly important hearing, at a time in the marriage, if you will, of facial recognition and AI, which we've all heard so much about in the last few months.

But we still-- if you ask anyone at-- except perhaps at the level of someone from a tech company or professors at Stanford or NYU in this, we have no real concept of how invasive this technology is. We just know that we have seen an extraordinarily troubling turn of events.

On November 27, 2022, as you discussed, my associate Kelly Conlon, was chaperoning her 9-year-old daughter's Girl Scout Troop at the Annual Christmas Spectacular show at Radio City Music Hall. Almost immediately after entering the building, she was confronted by two security guards. They handed her a one page notice and then proceeded to eject her in front of her daughter and her other girl scouts.

Unbeknownst to her Kelly had been flagged by a covert facial recognition system used by Madison Square Garden. What we have since learned is that although MSG claims to use this technology at its properties to promote the safety and security of its patrons, this is simply not happening.

Sadly, it appears that Ms. Conlon was identified by this technology because she was an employee of my firm and had therefore been put on a list that included several thousand lawyers from over 90 other firms. She was included on this list because my firm represented an individual in a personal injury case against a restaurant that was later acquired by Madison Square Garden.

It was a case that Kellie Conlon had absolutely no involvement in or knowledge of. MSGs use of facial recognition in this way has led to significant public backlash as lawmakers, civil rights advocates, and other members of the public recognize the serious danger posed by MSGs use of this rapidly evolving surveillance tool.

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

When you weaponize facial recognition, you invade our fundamental right to privacy, you stifle our freedom of speech, and Americans and especially New

Yorkers will not sit by and allow stadiums, theaters, or restaurants in their city to be cleansed of dissident fans or customers who pose absolutely no threat to the security of others.

In Kelly's words, she wants to take the humiliation she suffered, and her daughter suffered, and turn it into something positive. She is grateful that this council is taking a hard look at these dangerous and dystopian practices.

Thank you.

I know it's stunning. A lawyer finished two minutes ahead of time and is not arguing for more time.

CHAIRPERSON VELÁZQUEZ: I know.

MR. DAVIS: I credit that to your administration told me it was two minutes. So that's a great move.

CHAIRPERSON VELÁZQUEZ: Anytime. We try to be generous, though.

So we have a couple of just questions for those impacted. And we're just literally-- while your firm has been impacted, we just want to discuss, like Local Law 3, the one that we mentioned earlier of 2021, requires at all commercial establishments in New York City that are collecting, using, and

retaining biometric identifier information to disclose this to consumers. Do you think that this notice would impact your decision to enter commercial businesses that use this technology?

MR. DAVIS: Well, first of all, let me address-- the answer to that question directly is no. And I will tell you that we as consumers are simply not accustomed to reading the small print, looking at a sign that's perhaps written in legalese, or as in this case, signs written which simply don't disclose what they're really using the data for.

So I don't think it'll have an impact. And I'll tell you, it's-- it seems like a terrible price to pay that now, when we go to a public venue, when we go to a hotel: Registering at a hotel, if you look at the small print, it will tell you, without an opt out, that the hotel has different forms of -- they just call it surveillance cameras, and the footage that they obtain, they can use in perpetuity, for any purpose they choose, commercial. They can show it anywhere. They can use it for profit. And it would be, I think.

I think it would require some aggressive legislation to dissuade companies like MSG, and all

companies that are doing business in New York, from being sneaky and sly about this. And of course, all this happens at a time where-- how can you trust this technology? I mean, especially for minorities, how do you trust it when it has those rates of-- of error, of inaccuracy that all come down hard on minorities?

I think that the time for the use of these technologies perhaps has not come. And if it has come it must be restricted to security purposes only.

Now, you asked me a question about signage. And because of the timing of my presentation, I didn't present information about the signage. But let me tell you that after Kelly was ejected, I went over and looked at the signs.

As a matter of fact, I went over there with the intention of trying to experience what Kelly did when she was ejected. Fortunately, unfortunately, it didn't pick me up. I don't know why. I just walked in. I wasn't wearing sunglasses or a Groucho Marx nose, but I did look for the signage and the signage was inconspicuously posted. In other words, the signs were facing sideways. Then when I finally took a real good look at the signs, the signs only said

"for security purposes only." That's a misrepresentation. And the deeper that you dig into the facts surrounding not only MSG, but so many businesses, you're going to find that there is a pattern of deception, a pattern of-- You know, so few people read the signs, but the ones who do going into MSG come away with, you know, an impression that's totally inaccurate. I mean, their sign said, "Important notice. To ensure the safety of everyone in our venue, Radio City Music Hall employs a variety of security measures, including facial recognition, which uses biometric identifier information."

So, you know, we did challenge them on that, on the propriety of their signage and that was at Radio City.

And the MSG signage was a little different. It said, "Important notice, Madison Square Garden is a world famous arena, and in order to ensure the safety of everyone in our venue, we employ a variety of security measures, including facial recognition, which uses biometric identifier information."

And the correction that they made-- they recently made to bring their signage into compliance with Section 1202 of the city's law still, does not--

although it recites the magic words, it still does not tell you what they're using it for.

But I think as the facts emerge in this case, and I suspect they will, since there is quite a bit of litigation pending on many, many fronts from as far away as Delaware, and a shareholders' derivative action-- which I would point out, MSG is restricting lawyers who are involved representing MSG shareholders from going into the garden. But as this investigation unfolds, I think you will find that the proscription against sharing, trading, or otherwise using for profit has been violated. And the problem is that there is no transparency.

So, I don't know how to draft a law. But I know that the law must be very clear. It must provide for transparency. It probably needs a pack of watchdogs to cover this city. But I think that as a result of doing that, and I-- as I understand it, this is probably your fact-finding effort to take the legislation and find out if what you did back in 2021 is working, and see what you need to do to make it work, so that the public is aware of exactly what their biometric identifier information is being used for, how long it's being stored, who's storing it,

and in this case-- And this is not just an MSG issue. It's not an MSG issue. But I submit that if MSG can get away with this, then you are going to have a slippery slope of surveillance in the city, and New York, parenthetically, has the highest density of surveillance cameras in the country.

If MSG gets away with it, then our privacy is a memory of what life was like, maybe around the turn of the century, but not what it's like now.

CHAIRPERSON VELÁZQUEZ: Thank you. I have Councilmember Farias, who has a question for you.

COUNCILMEMBER FARÍAS: More like a question slash statement.

So facial recognition is like something that is, for me, really important to try to see how the municipality can have a major role in putting in protections for just citizens, for people that are going to and from businesses or concerts, and so I guess, for me, outside of the state and the city's role that you know, what we're trying to do here with putting in these laws or putting in these bans, or certain-- certain sorts of restrictions or limitations to where and how they could be utilized, what do you see as the City's role or the State's

role in even educating consumers and residents on what facial recognition is? You know, as we've been learning over the last several months, like, we have young people to older people alike that are using Tiktok, that it's very much a facial recognition AI, that is taking pictures and manipulating it, or taking your face and manipulating it, and storing it for later usage to be consumed in a different way. And so I've always thought of this on the aspect of-- or at least of the side of -- outside of all of the things where we are trying to be proactive on, instead of responsive to which we're already behind, so we're always going to be responsive to this -- What is our role, or do you see us having a role of any, and trying to inform the public enough that they can see how protective of their own-- of their own autonomy and this process be, if anything at all?

Mr. DAVIS: You brought up a really important point, and that is: Americans are oblivious. When we sign up for these apps, whatever they are, Tiktok, they're oblivious that corporations somewhere, maybe here, maybe in China, one of our political enemies in Russia, they have all of this data because it's so easy to get.

So parenthetically, when Dolan wanted to go after lawyers in an attempt to, I don't know, dissuade, a lot of litigation, which wasn't so successful, what he did was he went to our websites, and he scraped that information from us. And I can tell you what a dystopian experience it is when you are confronted at a venue by five or six security guards accompanied by a uniformed New York police officer, and they all have on their phones as they're surrounding you, they all have your picture which you recognize from your website. And then they proceed to ask you, "Is your name...?" Of course, my answer was, if you don't know my name-- they probably know what day of the week I was born on, and you know what car I drove to, to the venue.

So I think educating the public is critically important. In a way, it's almost like our protecting our environment. There are people who say, you know, it's too late. This is-- this is going to happen. And I-- By the way, I applaud what you're doing, because I learned so much from your hearing on the disposables about the-- about the Texas sized-- I learned so much about that it's changed my behavior.

Unfortunately, you can't just educate people and have them hear that the genies out of the bottle, all of this data, billions and billions of pieces of data, everybody in this country, they have a dossier on that is now accessible, using artificial intelligence in nanoseconds. You have to reinforce that, yes, we can do something. And doing something often has to take into account what the political realities are. And the political realities with facial recognition are that there are some big lobbies and many politicians who are going to listen to corporations, and not to consumers and workers, and they're going to fight it. And they are well-equipped to fight it, better-equipped to fight it on a federal level and on state level.

You have taken a bold move by being the tip of the spear. And the fact that you are bringing this to a head will mean that action will be done, whereas, for example, the state legislation which we don't have time to go into now: It's good, I mean, it's got a lot of great points, but the chances of it getting passed are a lot lower than what you're doing.

So I applaud you for that. And yes, your action, and your inquiry is critical in staving off this dystopian state, which we all hope is not progressing at the same speed that global warming is or faster.

CHAIRPERSON VELÁZQUEZ: Thank you so much for that. We appreciate you.

MR. DAVIS: Thank you.

MS. FOSTER: Good morning, and thank you to the Committee on Consumer and Worker Protection for holding this hearing today. My name is Meg Foster. I'm a Legal Fellow testifying on behalf of the Center on Privacy and Technology at Georgetown Law. The Center is a research and advocacy organization that works to expose and mitigate the disparate impact of surveillance technology on historically marginalized groups, and we have been studying face recognition for the past eight years.

Most of the efforts to limit or ban facial recognition to date have quite appropriately focused on its use by the government, primarily law enforcement, and the myriad harms stemming from that use, including but not limited to the wrongful arrest and incarceration of at least four black men. But in the absence of parallel efforts in the private

sector, face recognition companies have successfully pivoted to selling their products to businesses, thereby substantially shrinking the number of spaces in which we are not subject to a watchful eye.

With that in mind, there are three risks to consumers and workers that I'd like to highlight today.

First, as illustrated by the widely-reported-on incident at Radio City Music Hall, businesses can use face recognition punitively to ban from their establishments, anyone that they deemed to be an adversary, be it lawyers, whistleblowers, and former employees or public critics. Such practices are not only wholly contrary to free speech principles, but they discourage and impede the transparency and accountability needed to protect workers rights, public health and safety, and meaningful competition.

Second, businesses may also use face recognition to engage in unlawful discrimination. Profession may not be a protected class but the ability to categorically identify and exclude a group of people as MSG did and does suggests that that practice can indeed extend to those who are protected under New York State and City public accommodation laws.

Moreover, biases in face recognition software I first discovered over a decade ago still persist today, putting people of color, women, children, and the elderly at risk of being misidentified, and wrongfully denied access to services, products, and experiences. And that's not speculative that has happened.

Finally, the private sector lacks even the few legal safeguards that exist in the governmental context. Because businesses are subject neither to constitutional law nor public records laws, consumers and workers have scant opportunity to discover, let alone challenge, this invasive yet largely invisible technology.

Despite its proliferation, there is little evidence of face recognition technology provides any real benefits to society, including for security. On the other hand, there is a plethora of evidence that it causes serious and far-reaching harms. Left unchecked, the exclusion of high power attorneys from popular entertainment venues will be just the tip of the iceberg when it comes to businesses using face recognition for nefarious purposes.

For that reason, I urge the Committee to consider introducing, at the very least, legislation that prohibits the use of face recognition technology by New York City businesses. But ideally, together with the rest of the City Council a more comprehensive moratorium that addresses the uses and abuses of face recognition in all contexts.

I greatly appreciate the Committee's attention to this important matter. And thank you for your time.

COUNCILMEMBER MENIN: Thank you so much for your testimony. So since you, as you stated at the outset, have been studying this issue for a number of years, what have you seen successfully done in other jurisdictions legislatively?

MS. FOSTER: So there hasn't been a lot of success. As I mentioned, a lot of the bans and limitations have only been with government use. And that's one of the reasons we're here today because there are far too many loopholes for businesses. One state that has had success is Illinois with the Biometric Information Privacy Act. That has caused Clearview AI to actually virtually withdraw from the State of Illinois because that act requires consent from consumers before biometric information can be

collected, which is virtually impossible when you're engaging in persistent real-time surveillance.

CHAIRPERSON VELÁZQUEZ: What was that called again:

MS. FOSTER: BIPA, the Biometric Information Privacy Act in Illinois?

CHAIRPERSON VELÁZQUEZ: Thank you.

MS. FOSTER: Thank you.

COUNSEL SWAIN: The next two panelists can come up to the table, Nina Loshkajian and Jake Parker.

MS. LOSHKAJIAN: Okay. Can you hear me all right? Yeah. It's a very faint light. Good morning, Chair Velázquez, members of the Committee. My name is Nina Loshkajian, and I'm a Legal Fellow at the Surveillance Technology Oversight Project, or STOP for short. We are a New-York-City-based civil rights and anti-surveillance group.

I really appreciate the opportunity to testify today on the harms of facial recognition technology. And we are here specifically to urge the Council to ban the use of this discriminatory and invasive software in places of public accommodation.

At the outset, thank you so much Chair Velázquez for taking action, and for organizing this important

hearing. But generally, we are disappointed with the Council that this hearing is so narrowly focused, and that the Council is seemingly ignoring the threat of facial recognition in other contexts, as other panelists have mentioned, use by police, and use by landlords.

Public Advocate Williams, in his initial statement, mentioned that he had worked with us and other organizational partners to draft legislation that would ban the use of facial recognition in multiple contexts. And we're disappointed that we've been pushing that legislation for over a year and it is yet to be introduced or included in any agenda for committee hearings.

So it just seems like the Council keeps putting our privacy rights and our civil rights on the backburner. But we do appreciate this council-- this hearing being held today by the Council.

When it comes to business use New Yorkers should not be forced to hand over their biometric data just to pick up groceries or to go to a concert. As many have mentioned, facial recognition is biased and error prone. Because of the AI that it runs on being infected by human bias, it is much more likely to

misidentify a young woman of color than it is to misidentify a middle aged white man, and it is incredibly invasive to allow businesses to collect this data, making them extremely vulnerable targets for hackers, let alone, you know, allowing them to engage in selling this data to data brokers. And this tool with the bias built in, can and does end up in the hands of people with terrifying potential to misuse or abuse it.

As many have talked about, James Dolan is using it to seek vengeance against his foes, blocking access to ticket holders affiliated with law firms suing him. I'm not just concerned about this, because I'm personally a lawyer myself. It's easy to envision companies using this against workers more broadly, you know, barring whistleblowers from within their-- you know, employees within their business. So this is really a consumer and a worker issue. I want to highlight that.

Given the bias, invasiveness, and potential for abuse of facial recognition, it has no place in New York businesses, and yet it does.

Facial recognition is already harming New Yorkers, and it's used must be banned now.

As I mentioned, we are pushing bills to ban the use of facial recognition by police, other government agencies, by landlords, and by owners of places of public accommodation.

Our proposed legislation specifically prohibits places of public accommodation from using biometric surveillance tools and any information derived from biometric surveillance tools.

I just want to address there's been some discussion of the local law that was passed a couple of years ago, and that is not even an opt-in regime. You know, it's just making it a requirement for businesses to post, and we think our position at stop is that bills like that are relatively meaningless, because as a lot of previous panelists have mentioned, you know, a lot of consumers aren't aware of what they're reading, or how that data is actually being used. And so we think the only real answer here is a ban on use of facial recognition. That's the only way to truly protect New Yorkers. And this would prevent abuses like those we've seen at MSG.

So we're hoping for a hearing in the near future, and that Councilmembers will support our bills.

Again, thank you so much for this opportunity to testify and for holding this hearing.

MR. PARKER: Is it on there? Okay. Hi. I'm Jake Parker with the Security Industry Association. And thank you, Chair Velázquez and members of the-- of the committee here.

So our organization is a nonprofit trade association representing more than 70 companies, headquartered in New York, and more than 1300 nationwide. Our members provide a range of safety and security products and services throughout the US and the state. Among them are developers of facial recognition technology for wide variety of government, commercial, and consumer applications.

I was invited to provide some information on the business uses of this technology.

So starting with what the technology is: It's pretty simple. Software that matches facial images by comparing an image presented with one or more that has been enrolled in the system. This technology has matured, and it's proven to be incredibly useful across many different types of applications.

And I wanted to stop here and address the characterizations of the of the technology

performance that we heard about earlier in the hearing are just not accurate.

Two issues: One is the reference that was made to old research on face classification technology, gender classification, which is not matching. It's not facial recognition, and also reference to a four-year-old study from the government about the rate of false positives. That information is quite old now. But also, that same report said that the highest performing technology had almost undetectable differences across demographics. And the figure that we cited was literally the lowest-performing ones.

So if you look at the most recent US Government evaluation, you'll find the top 150 technologies are more than 99% accurate overall across black, white, male, and female demographics.

So considerations when implementing this technology are going to vary quite a bit, even including the privacy implications, depending on each specific application and its purpose. And SIA, we believe any advanced technology should only be used for purposes that are lawful, ethical, and non-discriminatory.

So for business use, in nearly all cases, they're utilizing this technology as a better way to accomplish a pre-existing underlying process of verification or identification that's already occurring through other less-effective means.

These purposes generally fall into two different categories: either enhancing business operations, or optimizing the functionality or security of products and services used by consumers. The vast majority of these applications are opt-in and based on prior consumer consent. So in my written testimony, I've detailed many different use cases for business, but I'll share just four here that are relevant to New York City, and used by businesses in the city that I'm aware of.

The first is access control. The technology provides a way for employees or other authorized individuals to securely enter a facility, speed through security checkpoints, and reduce touchpoints. We're finding a lot of utilization by large office buildings to address throughput issues at peak times. Also, we understand that virtual guarding at entry doors is an emerging use.

It is being rapidly adopted at major US sports entertainment venues to enhance fan experiences by enhancing mobile order pickup, age verification, streamline payment, and VIP access. The Cleveland Browns, and the Atlanta Falcons stadiums, and many others are already doing this. I haven't experienced this yet personally, but I'm looking forward to it, how many times have you missed a key moment in a sports game when you're waiting in line for food?

It has been used to also to provide credentialing for field access as well as locker rooms where it's not convenient for athletes to carry cards or keys.

When it comes to safety and security for customers and employees, businesses have a really serious obligation provide the most effective safety depending on your unique security risks. From office buildings to small venues like bars and nightclubs, to larger ones, using facial recognition as part of security screening offers advantages over the existing processes. It can cross-reference images with a limited gallery of known individuals known by the operator to provide alerts to staff for a wide range of purposes to protect occupants, such as controlling access when there's been threats of

violence, a protective order involving a specific individual. And this is important because individuals who are barred for security reasons are unfortunately very likely to ignore this policy and come anyway.

Additionally, as I think we know, retailers are getting slammed by organized retail crime and facial recognition is one of the key technologies available to stem this tide. The recent rapid growth in this crime is something we should all be concerned about. Retailers have seen about a 30% increase over the last year in this type of crime. There's a real human cost that extends beyond the initial victims, as the revenue from organized retail crime fuels drug smuggling, human trafficking, and other criminal enterprise enterprises, as well as the violence that comes with it.

So this technology can strengthen existing loss prevention programs as a theft prevention tool, and not typically for apprehension, which is important. When repeat offender interests a store, a manager receives an alert and they're able to approach the customer with the goal of offering excellent customer service rather than apprehending them. I recently

heard one report that this process was enough to help the retailer turn away a shocking 90% of their repeat offenders, and I've heard other reports that are very similar for around the country.

[BELL RINGS]

I will go and finish.

So just lastly, I'll add, we've done some public opinion research about this technology. The vast majority of Americans are supportive of using it in everyday applications. We found 70% are comfortable with its use to improve security at their workplace, for example.

And just one last thing I know we're talking about some additional policy proposals, but caution against overreach and restricting the use of technology is where this has happened. It's already been rolled back in some jurisdictions. Over the last year, the States of Virginia, California, the City of New Orleans, and the City of Baltimore, have all removed prohibitions on the technology.

I'm quite happy to answer any questions you have.

CHAIRPERSON VELÁZQUEZ: : You had mentioned early on. What percent of mis-identification is actual now? Because you said the rates that we were stating

were incorrect. And where are you drawing that information from?

MR. PARKER: Yeah, so it's important to distinguish here with-- with misidentification. I think usually what people were referring to when they-- when they say there are false positives, right?

So if you look back at the research that we cited, it's talking about gender classification software. It looks at a photo of a person and says this is a male, a female, or an approximate age, race, and other things like that. That's-- that's where that misidentification is assigning the wrong gender or the wrong, you know, attribute.

And so that's-- that's where that those figures come. As mentioned earlier, a 50 percent-- 50 percent error rate. That's-- that's where that comes from. As far as-- as far as the false positive rates. That is-- that is-- the US government measures all different sorts of performances on facial recognition technology. That's just one of them. More-- more commonly, the actual error is false negative, where-- A failure to match is a false

negative. So that's much more-- much more relevant to determining the-- how well the technology works.

I hope that helps.

CHAIRPERSON VELÁZQUEZ: How many providers are there of facial recognition technology that you are aware of?

MR. PARKER: So there's-- there's the providers of the core software technology, the algorithms, and then there's also-- so those that's one set. And there's other companies that are-- that are using those within other products.

But I'd say as far as the core-- the core developers, I think there's probably 20 or 25 that are the-- the leaders

COUNCILMEMBER FARÍAS: I mean, I'm like debating it. Yeah. I'm like having a hard time whether or not to ask any questions. But you made a statement, and I just want for clarification. You said in your testimony that you haven't been able to experience it yet, like at a game or at a concert.

MR. PARKER: Not myself, yeah.

COUNCILMEMBER FARÍAS: But you're excited to in the future. Respectfully like as a white man, like, I don't know if that's, generally, how the rest of

black and brown communities will feel about facial-- facial recognition technology being utilized in that way. Granted, I'm seeing a lot of different data here that you've listed, along with-- I mean, I guess my first question around enhancing business operations, what do you see that, or what does that mean, in a small local shop using facial recognition technology?

MS. PARKER: Well, addressing your first-- first point. What I was speaking about was an opt-in voluntary program, you could-- you could do-- you could enroll in as a fan--

COUNCILMEMBER FARÍAS: Yeah. Ultimately, like that's our problem, right? Like businesses, law enforcement, MSG, perfect example, are utilizing this technology without notifying people equitably in a real way, right? Even having-- I mean, we all see when we go shopping, there's always a store, whether they have a security camera, what type of it we don't quite know, we just assume it's a regular, you know, CCTV kind of thing, where it's recording for 30 days in the back of the room. We don't know where that data goes. No one really gets to opt in, to even just having a surveillance camera for theft, or

burglary or anything like that in a business. But this is like a different type of technology that people really don't quite understand. And while I can see some pluses for-- for businesses, and I'm trying to get from you what-- what is enhancing business operations, when you can facially recognize every patron that comes through your doors and every worker that you have? How is that what-- what enhancements are there? I feel like I have to be missing something.

MR. PARKER: Yeah, I'd say-- I'd say first of all, I don't think that's what happened-- what is happening, identifying everyone that comes through the door. That's not-- You know, that's-- that's not what's occurring. But I think-- so we would say that for-- for business and commercial use, there has to be a legitimate business purpose for the technology. That's-- we have a set of guidance implementation principles that we've publish.

So that's-- that's really the key. It needs to be-- I would say, it needs to be something that enhances the safety and security of the occupants of the areas being protected, or something that enhances customer experience and services.

COUNCILMEMBER FARÍAS: Okay. And then optimizing functionality and security of products and services-- and services used by customers. Is that-- That's like what you were relating to, like, theft, and, like, having repeat offenders coming in and out?

MR. PARKER: Well, no, I would say that's more business operations.

COUNCILMEMBER FARÍAS: Okay.

MR. PARKER: But as far as enhancing services, that's making sure that you can, for example, use-- use your-- use facial recognition as a form of payment, so you don't have to-- so it can speed up the process of paying for something. It also makes it so you don't have to expose other information, such as your social security number, you know, driver's license number, address, other things that actually are more vulnerable to abuse, if they are compromised. It saves you from having to provide that kind of information that would go to a database that then can be breached. So your biometric data, that's-- that forms a template from your face when it's used in matching by itself that is, is useless outside of the software that creates it. So if that data is compromised, it's-- no one can do anything

with it. They can't even recreate your photo from it.

COUNCILMEMBER FARÍAS: And in the survey, because-- and I plan to read the rest of it. I don't see any of the stats here with my quick scan. Do we know-- Do you have any-- like any data in your survey of businesses that are utilizing it, or companies that are utilizing it, and where they store data, what they've done with the data, what agreements they have with localities or states in terms of law enforcement usage, or other usages of their data?

MR. PARKER: So law enforcement use is really a completely different way of using the technology instead of considerations.

But I'd say, for the most part, this technology, when it's provided, it's-- there's a supplier, it's probably the end user. They're the ones that actually would populate the database and use it for their purposes. So the provider the technology is not holding that data usually. They might be hosting it in a private cloud or something like that, but they typically don't-- they're not the ones that are accessing it.

COUNCILMEMBER FARÍAS: So you don't-- I mean, you haven't surveyed anyone that-- on whether or not they have local agreements, or state, or city agreements with their local law enforcements. Because I-- because I am sorry, right before. I do think like, yes, we watch movies and we think it's super cool when you get to, like, get your face scanned to enter a room. Like people kind of associated sometimes in that way, right? There's no real connection sometimes in what this-- what this could mean for people. But really when it comes down to like nuts and bolts, what we see is we do see really vague, and-- and non-transparent connections to how the data is utilized, or municipalities have agreements with their law enforcements, with how businesses will need access, or not, to any of their capability of holding on to this data. So sometimes-- I mean, I'm not saying, like, every business is saying, you know, "Check yes. We're going to give up-- give up all of this." But sometimes the municipalities themselves will say, "Well, we need this because something happened, or because this is under investigation." So I'm just wondering if you

have polled anyone on what their responsibility is to that, and/or, you know, if they've had to do that.

MR. PARKER: So I'm not-- I'm not aware of any arrangements where a business would share the actual biometric data with law enforcement. That's not typically the way it works. They have, they might have photo evidence that comes--

COUNCILMEMBER FARÍAS: Sure.

MR. PARKER: --from an incident, and then the law enforcement does completely on their end, you know, as far as investigating that. So does that-- does that help?

COUNCILMEMBER FARÍAS: Yeah. Thank you.

COUNCILMEMBER MENIN: Good. Okay. Just a couple of questions on this survey. So one of the things that I see missing from your surveys, I don't see anything about surveying concert venues, sports stadiums. It seems that this poll is more geared to airlines, TSA, banks, and schools. Did you do anything more on other types of businesses?

MR. PARKER: Yeah. So what I provided in there is just a top-line summary. There's a lot of other data points in there. It's on our website, for the survey.

Also, I will mention it was done several years ago now. So that is actually one of the sort of newer emerging uses of the technology. It's-- it's sports and entertainment venues for fan experience.

COUNCILMEMBER MENIN: Right. That was going to be my second point. I noticed the survey is done from August 2020. And now, you know, three years later, when a very different world around facial technology, where now it's really exploded into these, again, concert venues, stadiums, places where people do not expect to have-- be surveyed and surveillanced by facial recognition.

So this survey three years ago, just seems not to be as on-point as what we're discussing today.

So you don't have any more recent data?

MR. PARKER: Not specifically on-- on sports venues. But I will say this: That that type of application that was mentioned before is not surveillance. That's a matter of using it to authenticate your identity for services. It's completely different than surveillance.

So-- and I also would say your-- you know, venues are using this-- this technology for security purposes. You know, every venue is going to have a

list of individuals that are-- that are prohibited. It doesn't matter where it is in the country. There's issues even, you know, a bar in a small town. You're going to have someone who is violent, or, you know, where somebody has said, "Look, you can't come back here."

So they're responsible to their patrons to protect them. And they're going to implement some kind of policy like that whether they have the technology or not. But if you're not-- if you're not in that category, you're not being surveilled, because there's no, there's no reference identity to match it with. Only the folks that are enrolled with their image on-- in that category can be matched.

COUNCILMEMBER MENIN: Okay.

CHAIRPERSON VELÁZQUEZ: So businesses like CLEAR, that are enabling us to beat the lines, right? Whether it's going into Yankee Stadium, or going to the airport. How do you see that continuing? And what are the benefits? But also, how do we ensure that that data is protected?

MR. PARKER: Yeah, so there's-- there's a lot of standard data protection techniques that a company will use to protect that. It was said earlier that

somehow it can't be encrypted. I don't know where that comes from. But usually the facial template is encrypted. And so, you know, that's-- that's one thing. Allowing you to verify your identity that wave speeds up the process. I know TSA is-- is expanding the use of its-- of the technology to be able to match you against your actual electronic photo on your ID which is more secure and faster.

In one example too, I don't know if you've ever tried to clear customs coming back from international trip or from a cruise. So I know a lot of the cruise lines now, and this is a CDP function, but they will allow you to clear customs using your face matched to your electronic-- electronically to your passport.

And the last time I did that, I think we got off the ship in like 20 minutes, and I remember it taking hours you know before that. So there's a lot of-- a lot of benefits there. And it's the same process you're doing, just instead of someone looking at it, you're having you know the machine match it. So-- and I know that the cruise lines are also starting to use, you know, on the private sector side they're using it as a way to access your count on the ship and pay for things on the ship.

CHAIRPERSON VELÁZQUEZ: I guess one of our more important questions, and I'm sure like we're hammering this, but how can we better protect our consumers from the misuse of this facial recognition technology, from commercial businesses?

MR. PARKER: Yeah, I mean, I guess-- I don't know. I don't have the answer to that exactly. But I know that there's-- you definitely have to start with the, with the biometric data law that you have here in the city, which is the first of its kind at the municipal level. It's the only jurisdiction I know of that requires a signage requirement, which I think is actually pretty important for transparency purposes. Maybe that could be-- that can be improved. And also, as was mentioned earlier, bars the sale of that biometric data collected, which I think is important. So...

CHAIRPERSON VELÁZQUEZ: Any more questions? Thank you so much. Thank you both.

Our next panel will be a Zoom panel. We'll be starting with Jeramie Scott. Then we will be going to Andrew Rigie. And then Daniel Schwarz.

Chair Velázquez and members of the Committee, thank you for this opportunity to testify today. My

name is Jeramie Scott. I am Senior Counsel at the Electronic Privacy Information Center, or simply EPIC, as well as director of EPIC's project on surveillance oversight.

EPIC is an independent, nonprofit research organization in Washington DC established to protect privacy, freedom, freedom of expression and democratic values in the information age. EPIC has paid particularly close attention to facial recognition, because it is a dangerous technology whose risks increase as the technology expands, whether that expansion is by the government or businesses. The technology poses a serious threat to our privacy, or civil liberties, our constitutionally protected rights, and our democracy.

Facial recognition has accuracy and bias issues that are most likely to impact marginalized groups, but even a perfectly accurate and unbiased facial recognition system poses a fundamental risk to democratic society when widely deployed. Allowing New York City businesses to freely implement the use of facial recognition as they choose would have a negative effect on the city.

There are two points in particular I would like to stress.

First facial recognition destroys anonymity and removes control of identity from the individual. It will become a de facto universal digital ID controlled by large corporations and/or the government. No longer will individuals have a say when they are identified. Identification will happen on a regular basis with or without your consent or even without your knowledge. A black box will be created around how companies use the massive amounts of identification data collected by businesses in New York City, and incidents like that which occurred at Radio City Music Hall will become more commonplace, and where you work, and among other innocuous factors could affect your ability to enter certain venues. Legislators who support a bill that a particular business does not like may find themselves unable to enter the venues that business controls. There'll be a record of everywhere you go to be aggregated and analyzed as some businesses fit.

The second point is that allowing businesses to freely implement facial recognition technology will create the infrastructure for mass face surveillance

that will undoubtedly lead to mission creep. Whatever the original purpose of the facial recognition, it will expand to other purposes, commercial as well as government, particularly for law enforcement. I urge the Council to take action on facial recognition and stop its unfettered expansion, and ban private entities from using facial recognition technology in places of public accommodation. But at minimal, the Council should implement a law similar to Illinois' Biometric Information Privacy Act that would prevent the use of biometrics on individuals without informed consent, limit the use of that data, and provide a personal right of action for violations of law. Importantly, such a law should make sure that people are not forced to consent either by not providing an alternative or making an alternative so arduous as to not be an actual choice.

Additionally, I'd like to agree with some of the previous witnesses who suggested that the Council should comprehensively address the use of facial recognition by not just businesses, but the government as well, particularly law enforcement.

And I'd also like to make a point related to something the previous panelist said about identity verification. I want to make clear that that can be a form of surveillance. In particular when that verification identity is kept on record. For instance, when you enter the airport, they're keeping that on record that you were at the airport at this time and you were identified. That is a form of surveillance.

But with that, I thank you for the opportunity to testify today and I'd be happy to answer any questions.

CHAIRPERSON VELÁZQUEZ: Thank you so much for your time.

COUNSEL SWAIN: Next will be Andrew Rigie.

MR. RIGIE: Hello, I'm Andrew Rigie, the Executive Director of the New York City Hospitality Alliance. Sorry, I'm not there. Interesting conversation about facial recognition. I'm actually going to speak about the other bill, Proposed Intro No. 8-A in relation to the disclosure of total ticket costs and advertisement. We think this is important to have these fees disclosed to consumers, but we do

think there are three important amendments we'd like to see to the bill.

The first one is we want to make sure that if a restaurant or a bar is selling a ticket to an event, the concert at their establishment, using a third party platform, that the business will not be held liable for violating the law if the third party platform doesn't provide the appropriate tech infrastructure to allow that restaurant, bar, or nightclub to disclose the total fees as required under the law, including the ability to separately list the various fees. You could probably go and look at language from the recent bill that was enacted, the Skip The Stuff Bill, which requires restaurants to only provide plastic utensils and condiments to customers upon request. There was a provision that was added to that, similarly, which essentially said if the third party delivery platform didn't allow the restaurant to comply, they couldn't be held liable. So we just want to make sure that that's addressed.

The second one, point in the proposal. It lists a maximum fine of $5,000. I think I saw Councilmember Menin here has a great bill that

addresses this issue, or what I'm going to get to, is we would like to see a minimum fine amount of say $100 added to this proposed law, essentially giving the administrative law judge a range that they can clearly use when they would levy any type of fine to a small business. You know, based on the situation, it can be different, and we want to make sure that the ALJ's have a full range based on the facts and relevant information of each case to be able to, you know, implement an appropriate fine amount.

And then the third and final one is something that we've just been seeking in all new rules, and already laws and rules that exist, which is to provide a warning and/or a cure period for all first time violations of this law. You know, there's 24,000-plus restaurants and bars. Many of them sell tickets at various times to different events. And they're not always scattered-- you know, going through city websites to learn about new laws and regulations. So in the chance there's a violation, especially one because someone didn't even know this was a requirement, they should be provided a warning and/or cure period in the law.

So those are my points. I'm happy to answer any questions, but we thank you for your consideration.

CHAIRPERSON VELÁZQUEZ: Thank you, Andrew.

COUNSEL SWAIN: Next will be Daniel Schwarz.

MR. SCHWARZ: Thank you very much. My name is Daniel Schwarz, and I'm testifying on behalf of the New York Civil Liberties Union. We thank the Committee and Councilmembers for holding this hearing and for the opportunity to provide testimony today.

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're 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 widely reported deployment of facial recognition at Madison Square Garden to ban people from the stadium that had already purchased tickets illustrates the dangers from the growing surveillance industry and the urgent need for comprehensive privacy protections.

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. In recognition of these harms, the City Council enacted Local Law 3 of 2021 as a first step to respond to the spread and use of these surveillance technologies and businesses.

Unfortunately, the law takes a rudimentary approach to biometric surveillance technology, merely requiring businesses to post signs advising that biometric data is being collected, but without requiring the provision of adequate information about the system, or the policies guiding its use. The NYCLU has repeatedly testified on this issue during the Committee hearing on October 7, 2019, and the subsequent hearing by the Department of Consumer and Worker Protection on the proposed rules on August 30, 2021.

We urge the council to establish the guardrails needed to protect against biometric surveillance technologies, which, at a minimum, require informed obtained consent, clear limits on the use, access sharing and retention, and mandatory security

standards, and explicitly ban the use of biometric surveillance in areas of severe power imbalance, such as when used by law enforcement, in housing, in employment, and in other areas where our fundamental rights are at stake.

A state bill, the Digital Fairness Act, Senate Bill 2277, Assembly Bill 3308, introduced by Assemblymember Cruz and Senator Kavanagh, serves as model legislation for comprehensive privacy protections and will ensure our anti discrimination laws and civil rights are not circumvented by digital means, prevent surreptitious surveillance, and create urgently needed biometric privacy protections akin to the Illinois Biometric Information Privacy Act, short BIPA, that were heard mentioned in earlier testimonies.

Enacted in 2008, BIPA stood the test of time, clearly illustrating that there's no substitute for individual informed obtained consent. It continues to offer crucial biometric protections that go [inaudible] far beyond [inaudible]. Powerful examples are the recent ClearView AI settlement that, amongst several other restrictions, prohibits the

vendor from offering the invasive product to private entities.

Nobody wants to live in a world where pervasive surveillance identifies them, tracks their movements and associations, and impacts which places they can visit, what services they can access, or how they exercise their free speech rights.

We urge the Council to take actions that meet these values and put an end to ever-expanding surveillance across the city.

Thank you very much.

COUNSEL SWAIN: Thank you. We encourage you to please submit your testimony in writing. There were some technical difficulties for a couple of seconds.

Our next panel will be a an online panel. We'll begin with Leila Nashashibi, Alli Finn, and then followed by Jason Berger.

MS. NASHASHIBI: Hi there. Good morning. My name is Leila Nashashibi. I'm very grateful to be speaking to you all today. I'm speaking on behalf of Fight For The Future in support of a policy to ban facial recognition, to protect consumers and workers.

Fight For The Future is a digital rights organization with over 2.5 million members

nationwide, including over 85,000 in New York City. Among other focuses we are leaders in the fight to ban facial recognition.

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

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

I'd like to speak a little bit to the impact of this tech on workers. It's an Orwellian tool that allows for constant surveillance of workers which can result in unfair hiring and disciplinary actions, often disproportionately harming black and brown workers. Corporations are using facial recognition

on workers already. It's replacing traditional time cards and is being used to monitor workers' movements and productivity. Uber Eats drivers have been fired because the company's faulty facial recognition identification software requires them to submit selfies to confirm their identity. When the technology isn't able to match the photos of the drivers, drivers get booted off the system and are on are unable to work, and thus unable to pay bills.

Amazon delivery drivers also have degree to AI surveillance, including facial recognition or lose their jobs. This is a violation of people's rights on so many levels. It's putting people in an impossible position, you know, giving up their most sensitive biometric data and their privacy, or facing you know, unemployment.

We can also be sure the tech will be used to suppress worker efforts to organize and engage in collective action.

For consumers, facial recognition is able to track people's every move, is able to create a digital map of where people go, what they buy, and who they interact with. Not only is that a huge invasion of people's privacy, but the data can also

be used to manipulate consumers through personalized advertising, convincing them to buy products that they wouldn't otherwise buy, for example, with sale prices.

The data can also be shared with other companies or law enforcement agencies. And because of the lack of laws protecting people from facial recognition, there's generally no way for folks to-- for people under the surveillance-- for people to know if they're under the surveillance, and no way to avoid it.

I'll also note that many of these systems say they pick up on abnormal movements as they track people, which puts neurodivergent people and people with physical disabilities at sort of a higher risk of being flagged and harassed by security guards.

I'll also note that banks are using facial recognition to verify identities and-- and could make judgments about who should or shouldn't get approved for a loan based on an algorithm that is totally secret. There's no oversight or opportunity to appeal. And stores are using facial recognition to scan people's faces and bar entry-- in some cases, bar entry to anyone who gets matched, for example, to

a mugshot database. And we know that because of the reality of over policing, and the prison industrial complex that targets black and brown communities, black and brown people are severely over represented in those databases. So it's basically outright discrimination against people of color, and it's as of now legal, and it's really easy to imagine additional ways that the tech can be used by business owners to target entire groups of people.

A lot of the threats to the general public have already been-- been touched on. I think that there was a previous comment regarding the security and safety of this data, the fact that it's-- it's more risky to have your social security number stolen. While of course it is-- it's dangerous to have your social security number stolen, when it comes to biometric data, that's data that cannot be changed, like a social security number expired and--

[BELL RINGS]

SERGEANT AT ARMS: Your time has expired.

MS. NASHASHIBI: Sorry, was that the end of my time?

CHAIRPERSON VELÁZQUEZ: Yes. If you want you can submit it, written testimony.

COUNSEL SWAIN: Next is Alli Finn.

MS. FINN: Hello. Thank you Chair Velázquez and everyone in attendance. My name is Alli Finn. I'm a Senior Researcher and Organizer with the Surveillance Resistance Lab, an NYC nonprofit organization that focuses on corporate and state surveillance systems as one of the greatest threats to democracy, racial equity, economic justice, and migrant justice.

Facial recognition technology, along with other biometric surveillance technologies are a monumental threat to democracy and to people's rights and security, not only their privacy. We are here today to call on the Council and the Administration for not only regulation and notice, but prohibition on the use of biometric surveillance technologies by private entities, specifically in places of public accommodation like theaters, restaurants, hospitals, hotels, stores, and public buildings, as well as strong limitation, again if not outright prohibition, on government use. Local Law 3 is not enough. It falls far, far short of even informed consent and opt-in policies, and even farther short from protections from permanent harm.

The MSG case is an alarming example of the weaponization of biometric surveillance technology, which is growing in use by not only corporations but also by government. Industry lobbyists, as we just heard, consistently spout increased accuracy numbers as a solution. This obscures that technologies, when accurate, are applied to identify and target people to protect corporate and government interest at the cost of people's liberties, rights, and security.

This is clear in the case of MSG, where the company used facial recognition tech to deny multiple consumers holding valid tickets entry to sporting events at performances simply because of who they work for. That can easily be transposed to other aspects of people's lives and identities.

For a sense of the bigger picture, over the past several years alone facial recognition systems in the United States have been used to criminalize people living in poverty, facilitate mass arrests, and incarceration of ethnic and racial groups, surveil demonstrators exercising their First Amendment rights at protests, and target immigrants for deportation.

Companies like MSG entertainment and the unnamed vendor providing their facial recognition systems

have virtually no restrictions over how they treat facial scans and all the other data they collect, almost no required disclosures at the local state and federal levels. As far as we know, they can keep the data indefinitely, and we have no idea who has access to it, who it is shared with or sold to.

Local Law 3 unfortunately does not fix this. We cannot trust these companies to prioritize our rights over their profits, and urgently need regulation and prohibition.

I also want to point out that identity verification is also a form of surveillance, and for over 20 years, the industry has promoted invasive data collection and sharing underneath that banner, underneath that terminology of identity verification, claiming otherwise.

Proponents of facial recognition tech and biometric surveillance argued that it keeps people safe. But time and time again, we instead see that these technologies and their use puts people at increased risk of violence and denial of basic rights and resources. The MSG case also shows how easy it is for companies and law enforcement to justify their use of invasive biometrics by claiming public safety

concerns. For example, the lawyers denied entry to sports games and Rockettes performances did not pose a threat, and yet MSG used the same system supposedly implemented for consumer safety to identify and remove them.

Surveillance technology and algorithms, time and time again we need to repeat, are not neutral. They will always reflect the biases and the use of people who make them and the systems that use them, and they require prohibition, at the very least limitation.

Advocates have already been working with city Councilmembers to draft bills, including many of us testifying today with the Ban The Scan campaign, and others. We call on the City Council to engage with advocates and community members whose lives are deeply impacted by biometric surveillance technologies, and pass legislative-- legislation, excuse me, restricting corporate and city agency use of biometric surveillance to protect New Yorkers from permanent harm.

Thank you.

COUNSEL SWAIN: Thank you. Next will be Jason Berger.

MR. BERGER: Hi, good morning, Council Chair Velázquez and Councilmembers. My name is Jason Berger. I'm speaking on behalf of the Coalition for Ticket Fairness. Thank you for the opportunity to speak with you today, and thank you Councilmember Brennan for arranging this hearing and attention to this issue.

The Coalition for Ticket Fairness has been working with government bodies in New York and Washington for almost 30 years. We promote fan-friendly legislation and live entertainment ticketing in an ever growing and complex marketplace.

In my over 30 years on the issue, I've seen many changes and nothing draws from the basic concept that people love that live entertainment, and the ability to access it in a fair fashion is core to its success. The live entertainment ticket industry has grown into a very complex, non-consumer-friendly, myriad of exclusive agreements between venues and ticketing giants like Ticketmaster, AXS, and others. Outdating technology that creates issues with online distribution of these channels has led to customer dissatisfaction.

Regarding item 8-A, the fees on online ticket sales and in person are a very important issue which we completely support. But there are also issues such as disclosure of availability, restrictions on purchasing tickets without fees, public awareness on when and how many tickets are available, and most importantly, how a sale is final and a fan has limited opportunity in some cases to sell or transfer their tickets.

To the point of disclosing the fees we believe all fees should be made available to consumers without having to enter personal information. These details are collected and used for marketing and other purposes and should not be required in the ticket price and fee disclosure page.

For print or social media advertising, we believe it may be challenging to list all the prices, as many events have dynamic pricing models and pricings change constantly.

One thing that would be helpful however, is providing consumers with a way to purchase tickets without fees at box offices which are sometimes restricted from sales on the day that the tickets are made available.

Thank you very much for the opportunity to speak with you and I invite any questions.

COUNSEL SWAIN: Thank you. Our next panel will also be a Zoom panel. We will be starting with Tom Ferrugia, then James Sullivan, last Haba Scho.

MR. FERRUGIA: Hi, good morning. Good afternoon. Hi, I'm-- I know we're running late, so I'll move as quickly as I can. I'm Tom Ferrugia. I'm the Director of Governmental Affairs with the Broadway League. We are the trade association for the national theatrical industry. We have over 700 members nationwide, with over 400 maintaining offices here in New York City. Its producers, general managers, theater owners, everyone who works together to bring Broadway to New York City, and of course, Broadway around the world.

So I just want to thank the Committee for allowing us this opportunity to speak on what is obviously the less-controversial issue of what you're dealing with this morning. And I'll jump right into my statement. I have submitted my full statement for you to review. I'll just jump into sort of the main points. And then of course, I'm available for-- for any questions.

So given that the state legislature recently examined this issue in great detail, in consultation with many of the stakeholders, including the Broadway League, through revisions to the New York State ticket resale law, which was signed into effect for 2022 and does not expire until 2025, we strongly recommend that the Council defer to state law at this time without introducing further changes and additional complexity to the disclosure requirements-- tickets disclosure requirements.

The League has always strongly supported transparency and ticket purchasing process to ensure that consumers are aware of the source, price, and fees associated with their purchases. During last year's discussions, we advocated for state lawmakers to implement improved consumer protections, including enhanced market transparency, for all tickets sold to live events. Under a state law passed in 2018, online ticket resale sites were required to disclose in a clear and conspicuous manner, the total price of a ticket and how much of that is made up in service fees before sale is completed. More recently, Governor Hochul signed into law several additional amendments. She signed that into law on June 30,

2022, including a mandate that all ticket sellers provide the total costs displayed in the ticket listing prior to the ticket being selected for purchase.

Accordingly, we would propose that the Council allow ticket providers sufficient opportunity to comply with the new state mandates before evaluating whether additional regulation may be necessary. Intro 8 introduces significant compliance challenges with respect to digital advertising; open-ended runs with varying prices, as is common with Broadway; multiple distribution outlets, promotions, and dynamic pricing.

Implementing these changes while Broadway is still struggling to return to pre-pandemic levels would be extremely challenging. We're grateful to the Council for its continued effort to take an active-- continued active interest in the health of the live entertainment industry. However, we maintain that the State satisfactorily addresses these concerns about consumer cost awareness. And the changes made to the law in 2022 need time to play out before the city advances further alterations to the sale of tickets for live entertainment.

Thank you for this opportunity. And again, I'm available for any questions.

And I would like to add that if there is discussion about moving this legislation forward, we would like to be engaged in those conversations in order to address those issues that I mentioned, particularly with respect to compliance. With the way Broadway does business which puts tickets on sale for six months or a year in advance through, as I mentioned, multiple distribution at outlets, various-- prices change throughout the sale, because of dynamic pricing based upon selling. It's a very different model than when you have a one, or two, or three-night engagement. And we would like to make sure that the way we sell our tickets is part of the conversation to ensure that we can comply with whatever version of this law ultimately gets passed.

But again, our recommendation would be to give the state law some time for us to implement it and see how it affects buying habits before making any additional decisions about additional regulations. Thank you.

COUNSEL SWAIN: Thank you. Next will be James Sullivan.

Thank you Madam Chair and members of the Committee for letting me participate in this important conversation about biometric technology. I am BIO-key's Senior Vice President of Strategy and Compliance as well as Chief Legal Officer. BIO-key is a New-Jersey-based provider of identity and access management solutions that leverage biometrics in, we think, a positive way. We use it to get rid of the storage of passwords and to stop hackers from being able to take over people's accounts online.

But another way we use biometrics is to simplify how people are able to get to the workplace applications and be able to get in as if there was a doorman to let them in as opposed to having to find a remember some way of proving who you are.

We also allow consumers to secure their digital identity so that only them and not others who even are family members who might know all of their out of wallet ID verification questions cannot access and take over their identity without their consent.

I've worked in the biometrics industry in technologies for over 20 years, and I'm an attorney, member of the Georgia Bar, Privacy and Technology Section, and was a contributing member of the Sedona

Conference's Biometric Privacy Law Working Group, which aimed to help develop a model uniform template for biometric privacy laws nationwide.

I am techie lawyer with a computer science degree from Brown, and I really believe in this technology. And that's why I'm here today to help shed some light and answer questions about how the technology can be a positive, even helping with equity, as opposed to its perception as being something used for nefarious purposes.

BIO-key is a member of the International Biometric Industry Association, which is an industry group of responsible biometric technology vendors. They do exist.

We don't develop surveillance technology or facial technology, we develop fingerprint authentication technology. And we do include facial recognition software from a third party in our products, with user consent, in order to secure access to computer systems in a simplified way.

What I hope to convey in the next few minutes is that this is a charged topic, and there's really three several things to take away from a careful analysis of it.

First of all, biometric technology is very often misunderstood, and as a result, it's subject to sometimes unwarranted demonization. It works in a mysterious way. You suddenly are identified without having to say or provide anything.

This biometric testing, as was alluded to by the gentleman from SIA, is a test it's open to all players who want to submit their algorithm. Therefore, out of the several hundred algorithm submissions that have been tested, you're going to have both good algorithms, and many that are not ready for primetime. Unfortunately, what we hear and even heard today is that the NIST report, or a federal report, found that most spatial algorithms exhibited bias against people of color and other disadvantaged groups.

Unfortunately, that isn't-- Or I should say, fortunately, that isn't true of the majority of the quality algorithms that are in use by responsible people using this technology, whether it's government or in commercial settings.

The next thing is to consider a balancing of interests between individual privacy rights, which are absolutely paramount, and the right to, as a

business know who you're dealing with, and to not be subjected to the fact that somebody can essentially use anonymity to commit fraud or theft or other, really, breaches of the business interests in this case that was raised by several of the speakers.

If you must regulate, prohibit the wrongful conduct in the misuse or careless use of this technology. Prohibit the fact that it can't be used without adequate consent, if it's going to be used in the way that we do, or notice if it's being used in a method of surveillance, and tailor your restrictions to the problems that arise from the use of the technology, and not simply banning the technology itself.

I can expand on these points, and I will in my written testimony. But it's important to understand that biometrics are not vulnerable in the same way as passwords, or credit cards, or social security, to disclosure. And this is something that unfortunately leads to a great deal of misinformation. People believe that if a biometric is disclosed that you can't reset it, and therefore you're stuck, and you'll be subjected to identity fraud for life. Biometrics does not base itself on security. It

bases itself on integrity in order to make sure that you're actually measuring a real person and not going to be subjected to somebody who has the information, the measurements, and being able to inject them into an authentication or identification process and become you, in a digital sense.

That ability to have your biometric essentially tie things to you as a positive in the sense of protecting your assets, your 401k. Your-- your digital online assets and identity are protected by having a biometric associated with you. And the belief that somehow a biometric is like a password where, if it's disclosed, you're really just ruined--

[BELL RINGS]

SERGEANT AT ARMS: Time expired.

MR. SULLIVAN: --in your ability to protect your identity is a fallacy.

I'm open to any questions. And thank you. And I will submit this testimony in writing.

CHAIRPERSON VELÁZQUEZ: I certainly do have several questions, right? In your experience, you have said that you have seen it work for the good. Now in New York City, and various people who have

testified today have shown where businesses can take it another level and use it to their own detriment.

What do you see there? And how can we protect folks, consumers?

MR. SULLIVAN: Well, it's like many things in life that have positive applications and negative applications. And the answer is not to remove or throw the baby out with the bathwater, as they say, and say that you just can't use this technology. I believe that you can identify the misuses that can arise through the use of this technology, one of them being to select technology that does not exhibit the biases in the algorithm testing that NIST has conducted, make it so that people have a duty to do due diligence and incorporate technologies that don't exhibit those racial biases that will create bad outcomes.

I think you can also legislate that data shouldn't be sold, or that data shouldn't be used to discriminate in a way that you wouldn't allow discrimination if somebody had the personal knowledge of the individual. So for example, if you want to legislate that somebody cannot prohibit someone from entering a facility, then do it based on whether

they're using a biometric to do it, or whether they personally recognize or have a handbook of "watch out for these people."

Those are the kinds of conduct-based regulations that I believe you can apply to biometrics, that makes it so the technology can be used for good, and that where somebody wants to apply it in a way that has an overall malicious intent or bad outcomes that you can regulate narrowly, in order to be able to control that. And that's really the ultimate goal of government is to provide narrow-enough regulations that it doesn't overreach and start to essentially prevent people from being able to get the benefits of this technology, leading among them as the consumers that really benefit from having the ability to secure their own identity.

CHAIRPERSON VELÁZQUEZ: Perfect, thank you.

COUNCILMEMBER BREWER: I want to-- I'm sorry.

CHAIRPERSON VELÁZQUEZ: I have Councilmember Brewer here, who may have some questions for you. Okay?

MR. SULLIVAN: Sure.

COUNCILMEMBER BREWER: Thank you very much. I apologize. I was at another hearing. I'm so sorry.

So it's my experience that those who live in apartment buildings, I have had tremendous complaints when the owner wanted to use facial recognition. And I have been able to, with attorneys, get rid of that opportunity to open the building. These are primarily low-income tenants. These are primarily privately-owned. These are primarily rent-stabilized and rent-controlled. And lots of families, and children, and guests, and grandparents, and three generations living in the buildings.

So it was complicated to start with in terms of usage. It was complicated, because people feel that they're being watched. It was complicated, because often these are primarily families of color, and they felt that the recognition wasn't appropriate.

So there were enough-- there were no end to the questions.

So my question to you, is this a common complaint? Is this something that can be addressed? I must admit, it certainly didn't make sense for me to be using it at the-- at these buildings. I have three buildings that had to get attorneys in all cases, and we were able to squash this type of technology.

So I wanted to get your opinion on that.

MR. SULLIVAN: Well, I think anytime you're applying a technology that is-- if it exhibits a disparate outcome, then you want to question whether or not it's a fair application of really any technology.

If, for example, if you hired a security guard who had a personal bias, and they just tended to stop a certain group more often, then you would have issues with the conduct of that security guard. Ultimately, Biometrics is really trying to replace the process that people have done for centuries. They-- they look at a photo ID, they look at you, and they determine that it's a positive match or not. And unfortunately, a lot of those human manual interactions wind up having a bias or an outcome that is disparate across groups.

In the proper application of biometric technology, where there is not a bias in the underlying algorithm, then you actually get better equity, because ultimately there should be no distinction between how one group is-- is perceived and processed to be able to be admitted or not versus another. And, again, a biometric technology should

be evaluated based on its performance in those ways, as opposed to simply saying that because there are some, I'll call them bad apples, but really more-- more likely research projects that are in the NIST test results, that really weren't properly prepared to do that sort of demographic performance, those products are now being used to paint the quality products that are out there that do not exhibit these characteristics.

So I think there's a separate question of whether or not people are comfortable with the idea that you have to use something like this in order to get into your building. And we as an industry association, the [inaudible] always recommends that you give people the option of being able to opt out in a meaningful way, so that they can choose to say, "No, I'd rather just have a card and use a card to get in." But for those that benefit, just like E-ZPass, right? E-ZPass brought the ability to just drive through a toll booth. A lot of people were concerned that there was a privacy implication, the government can track you.

Ultimately people should have the individual choice to be able to say whether or not they-- they

want to leverage technology like this and be able to then get the access and the ease of use that it does bring, while others can choose to not do it, and do it in an alternative way and method.

COUNCILMEMBER BREWER: All right. Thank you very much Madam Chair.

COUNSEL SWAIN: Thank you Next we will have Haba Scho.

MS. SCHO: My name is Haba Scho, and excuse my English. I speak French, but I'm going to try my best.

CHAIRPERSON VELÁZQUEZ: Je parle Français alors.

COUNSEL: Okay, while we wait to see if they're able to rejoin, I'm going to call an in-person panel, Attiya Latif.

Good morning and thank you for having me here today. My name is Attiya, and I'm a Staff Organizer at Amnesty International USA. I run our New York Ban The Scan Task Force, and I'm here to speak about facial recognition technology.

The only adequate facial recognition policy is a ban. While the city has moved towards disclosure requirements for businesses, these are meaningless without clear opt-in procedures for individuals to

give consent for the extraction of their biometrics. Without this New Yorkers risk being subjected to mass surveillance.

The NYPD and business surveillance machineries across the city disproportionately threaten the rights of New Yorkers of color. The expansive reach of facial recognition technology leaves entire neighborhoods and protest sites across the city exposed to mass surveillance, while also supercharging existing racial discrimination.

From our research, we have found 25,500 public and private cameras across the city. Cross-referenced with the NYPD own stop-and-frisk data, we found that New Yorkers living in areas at greater risk of being stopped are also more likely to be exposed to facial recognition technology. This is predominantly black and brown people.

Even in their homes -- namely in the Bronx, Queens and Brooklyn -- communities of color face greater threats to privacy. We and our friends in the Ban The Scan Coalition have said this before: Even when it works facial recognition technology exacerbates discriminatory policing and prevents the free and safe exercise of the right to protest

through the chilling effect. That it is by design a technology of mass surveillance and antithetical to human rights, as we've already seen in cases of black and brown New Yorkers, against whom we suspect FR has been used.

That is why Amnesty is asking you distinguished Councilmembers to advocate for New Yorkers, New Yorkers of color, your neighbors and constituents, by working towards a comprehensive ban on the deployment of facial recognition in the city as the ultimate goal. The discussion about Madison Square Garden is just the first stop and a much longer conversation. We cannot wait till individuals are wrongfully arrested, unduly surveilled en mass, virtually lined up and used as experimental sites for potentially racist, invasive, and violent technologies.

Meaningful regulation and accountability cannot be replaced with modest transparency policies. Thank you.

COUNSEL SWAIN: Thank you. This is to confirm that we are not able to have Haba Scho rejoin us on Zoom before the conclusion of this hearing.

[GAVEL]

C E R T I F I C A T E

World Wide Dictation certifies that the foregoing transcript is a true and accurate record of the proceedings. We further certify that there is no relation to any of the parties to this action by blood or marriage, and that there is interest in the outcome of this matter.

Date 02/27/2023