CITY COUNCIL
CITY OF NEW YORK

---------- X

TRANSCRIPT OF THE MINUTES

Of the

COMMITTEE ON TECHNOLOGY JOINTLY WITH
COMMISSIONER ON CIVIL AND HUMAN
RIGHTS

---------- X

May 3, 2023
Start: 1:16 p.m.
Recess: 5:52 p.m.

HELD AT: COMMITTEE ROOM – CITY HALL

B E F O R E: Jennifer Gutiérrez, Technology Chairperson

Nantasha M. Williams, Civil and Human Rights Chairperson

COMMITTEE ON TECHNOLOGY COUNCIL MEMBERS:
Shaun Abreu
Ari Kagan
Robert F. Holden
Julie Won
Kalman Yeger

COMMITTEE CIVIL AND HUMAN RIGHTS COUNCIL MEMBERS:
Rita C. Joseph
Christopher Marte
Kristin Richardson Jordan
Rafael Salamanca

A P P E A R A N C E S

Michael Fitzpatrick, New York City Chief Privacy Officer

Ryan Birchmeier, Deputy Commissioner of Office of Public Safety from the Office of Technology and Innovation

Hillary Scrivani, Senior Policy Counsel at the New York City Commission on Human Rights

Daniel Schwartz, New York Civil Liberties Union

Albert Fox Cahn, Executive Director of the Surveillance Technology Oversight Project

Alli Finn, Surveillance Resistance Lab

Lisa Meehan, Mobilization for Justice

Robert Tappan, Managing Director of the International Biometrics and Identity Association

Jake Parker, Security Industry Association

Jay Peltz, General Counsel and Senior Vice President of Government Relations for the Food Industry Alliance of New York

Francisco Marte, President of Bodegas and Small Business Association

Stuart Reid, Co-Chairman of The Smart Community Initiative

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

Adrian Gropper. I'm the Chief Technology Officer of the Patient Privacy Rights Foundation

Jake Wiener, lawyer at the Electronic Privacy Information Center

Elizabeth Daniel Vasquez, Director of the Science and Surveillance Project at Brooklyn Defender Services

Adam Roberts, Policy Director for the Commissioner Housing Improvement Program

Avi Kaner, owner of the Morton Williams Supermarket chain

SERGEANT-AT-ARMS: This is a microphone check for the Committee on Technology joint with the Committee on Civil and Human Rights located in the Committee Room, recorded by Nazly Paytuvi on May 3, 2023.

SERGEANT-AT-ARMS: Good afternoon and welcome to today's New York City Council hearing for the Committee of Technology joint with the Committee of Civil and Human Rights.

At this time, please silence all electronic devices.

If you would like to submit testimony, you may at testimony@council.nyc.gov.

Just a reminder, no one may approach the dais during any point at this hearing.

Chairs, we are ready to begin.

CO-CHAIRPERSON GUTIERREZ: Good afternoon. I'm Council Member Jennifer Gutiérrez, and I am the Chair of the Committee on Technology. I want to welcome you all to our hearing.

We are pleased to be joined today by the Committee on Civil and Human Rights Chaired by my friend and Colleague, Council Member Nantasha Williams.

Today, we will focus on the use of biometric identification systems in New York City. The hearing will also focus on the following two bills, Intro. 1014 sponsored by Council Member Shahana Hanif prohibiting places or providers of public accommodation from using biometric recognition technology and protecting any biometric identifier information collect. Next, Intro. 1024 sponsored by Council Member Carlina Rivera limiting the use of facial recognition technology in residential buildings, and we will also hear Resolution 296 sponsored by Council Member Althea Stevens establishing a task force on missing women and girls who are black, indigenous, and people of color.

We are here today to address an invisible but urgent issue that affects all New Yorkers, the use of biometric surveillance technology in New York City. As we continue to evolve technologically, it is critically important to ensure that our laws and policies keep pace with these advances and particularly to protect the civil and human rights of all individuals. Biometric surveillance presents a unique challenge in this regard, and it is our

responsibility as elected officials to thoroughly examine its potential benefits and risks.

In recent years, we have seen a proliferation of biometric surveillance technologies in our city including facial recognition software, fingerprint scanners, and iris scanners. These technologies have the ability to collect vast amounts of personal data on individuals including their physical characteristics, behavioral patterns, and even their biometric identifiers. In many cases, individuals are not opting in for this data to be collected about them. With cameras installed in nearly every corner of the city, including retail stores, concert halls, and street corners by hundreds of different owners including New York City, the potential for misuse of this data is profound, and it is critical that we establish robust safeguards to protect against abuse.

Facial recognition technology and other biometric information systems are constantly evolving and improving, but their accuracy and potential biases are still a cause for concern. As such, it’s important that we implement reasonable and effective safeguards to minimize these concerns including

privacy issues, security breaches, and discrimination.

As we continue to grapple with the complex issues surrounding biometric surveillance, we must ask some fundamental questions. How do we balance the need for public safety with the need for individual privacy? How can we ensure that these technologies are used in a manner that is transparent and accountable, and how can we protect against the misuse of the vast amounts of personal data that they collect? How can we best implement the advice of experts who are warning about the proliferation of AI technology that is intertwined with this kind of surveillance?

These are challenging and complex questions, but they are essential ones that we must answer to move forward safely and equitably. I am committed to working with my Colleagues on both the Technology Committee and the Committee on Civil and Human Rights to explore these issues in depth and to develop policy solutions that reflect the values and concerns of New Yorkers.

Oversight hearings like this one are increasingly important to protect citizens from an

omnipresent, unregulated technology that hides in the shadows and benefits from a general lack of awareness and understanding about the ways in which it can flourish, profit off of, or hurt people.

Our goal today is to gain a better understanding of how this technology and the data it collects is used in our city and start to discuss what the best path forward looks like. We look forward to working with the Administration to mitigate any negative impacts that this technology may have on our communities. We're also excited to hear from industry experts and community advocates whose testimonies will be crucial in understanding the current issues and building better solutions. Let us work together to ensure that facial recognition technology and biometric data is used ethically and responsibly in New York City.

I'd like to recognize Members of the Technology Committee who are present today, Council Member Holden, Council Member Abreu, and Council Member Paladino.

Now, I'll turn it over to Council Member Williams.

CO-CHAIRPERSON WILLIAMS: Thank you. Good afternoon, everyone. My name is Nantasha Williams, and I serve as Chair to the Committee on Civil and Human Rights.

This afternoon's hearing is one that I've been greatly anticipating. The role that biometric technology plays in our lives has changed in a multitude of ways over the years. From the early days of automatic photo tagging in social media to being able to unlock our personal electronic devices with one look, it's safe to say the rapid advancement of this technology has played a part in its wide usage. This use is not limited to our own personal devices but also includes usage by businesses, public and private spaces, and residential homes and areas. It begs important questions such as who is holding onto the information collected by these systems and what can they use it for, was it developed with equity and accuracy in mind. Biometric identification often comes under intense scrutiny, especially facial recognition technology, which can have major civil and human rights implications. Of the main biometric identifiers, facial recognition is said to be the least accurate. Accuracy rates are the lowest when it

comes to identifying women of color but the highest when identifying white men. Despite these issues, facial recognition technology is used widely by different individuals, groups, and organizations, and it is estimated that one and two American adults is in a facial recognition database used by law enforcement. This inaccuracy and collateral consequences of using these technologies are issues I hope we'll get to discuss during today's hearing.

I'm excited to be joined by my Colleague, Council Member Jennifer Gutiérrez, Chair of the Committee on Technology, and, as she just mentioned, today we'll be hearing two bills aimed at protecting the privacy of New Yorkers in the face of an ever-advancing technological landscape. While I have questions and concerns surrounding the regulation and usage of biometric technology in our city, especially in the context of discrimination and privacy, I am also aware of its potential to be a useful tool in protecting businesses and homes. This type of technology can even be used to help track and locate missing people, something that is on my mind today as we also prepare to hear Resolution 296 sponsored by Council Member Althea Stevens. This Resolution calls

on New York State Legislature to pass and the Governor to sign legislation which would establish a task force on missing women and girls who are black, indigenous, and people of color. As we consider the advantages and disadvantages of this technology, it will serve us all to keep in mind its potential for good as well as potential for misuse and evil.

I will now turn it over to my Colleague, Council Member Shahana Hanif, for her opening statement on her bill.

COUNCIL MEMBER HANIF: Thank you to Chairs Gutiérrez and Williams for holding today's important hearing and for including my bill, Intro. 1014, on today's agenda.

I was proud to introduce this bill last week alongside Chair Gutiérrez, Council Member Rivera, Chair Williams, and Council Member Sanchez. I'm grateful to Council Members Louis, Marte, Farias, Richardson Jordan who sponsored the bill as well.

Currently, the only protection against the private sector's use of biometric surveillance technology is the disclosure requirement established by Local Law 3 of 2021. While an important step, this is insufficient in protecting the privacy and civil

liberties of New Yorkers. Under current law, as long as a business puts out a sign saying biometric identifier information collected at this location, they can collect the facial recognition data of every person who walks through their doors then use that data to discriminatorily prohibit entry and sell the data to third-party companies for a profit. We've seen the inevitable civil liberty violations that occur as a result of our lenient laws recently at Madison Square Garden which has been using facial recognition scans to bar entry to employees of law firms who are suing them and assign additional security to Knicks fans who criticize owner, James Dolan. While very disturbing, this high-profile story only scratches the surface of the potential dangerous uses of this technology in the private sector.

For example, a retail store could refuse entry to a shopper because their facial recognition system incorrectly determines that the shopper is a person accused of shoplifting. Studies have repeatedly shown that this false match situation is more likely to happen to people of color, women, trans people, and young people. Or a company could sell the biometric data it collects from unknowing

people at New York City stores to a government which could, in turn, use this data to help ICE carry out its cruel deportation machine. As a Muslim New Yorker who grew up in the post-9/11 era, I am all too familiar with the impacts of excessive surveillance. This is a basic civil liberties issue that our Body has a responsibility to take on.

Intro. 1014 would prohibit businesses from using biometric technology to identify or verify a customer. This would fully ban biometric technology being used in the ways I've just described, preventing discrimination and affirming our ownership of our own private data. While this bill is monumental, I want to emphasize this is not unprecedented. Portland, Oregon has passed and successfully a similar ban. Intro. 1014 exempts businesses that truly need to use biometric technology to carry out core functions such as ophthalmologists from this ban. This exemption explicitly does not apply to stores who want to use biometric technology for the purposes of loss prevention. While our city does need to address the issue of retail theft in order to help our businesses thrive, this harmful technology is not the way to do

it. As evidenced by the relatively limited use of this technology in the city, it is not an essential security tool. I want to be clear that typical tools like video monitoring are not impacted by this bill.

The bill does allow for the collection of biometric data under very limited circumstances such as a customer proactively opting into the Pay by Palmprint Payment mechanism at a grocery store. Under the bill, a company would have to receive written consent from the customer before collecting the data, and service could not be denied to a customer who rejects data collection.

For cases in which a customer consents to data collection, the bill establishes the following important consumer protections:

One, the customer would be allowed to ask for data to be deleted at any time.

The data would have to be deleted after its initial purpose is served or after two years, whichever comes first.

Third, the company would be required to publicly share its data retention schedule.

Fourth, the company would be required to implement safeguards to prevent data from being stolen.

I want to thank the incredible Ban the Scan Coalition who we just rallied outside with and who are here to testify in support of Intro. 1014. The Coalition includes racial justice leaders like the National Action Network, civil and human rights institutions like NYCLU and Amnesty International, decarceration advocates like Freedom to Thrive, and technology experts like STOP and Fight for the Future. The broad diversity of supporters speaks to the harm that biometric surveillance creates and how urgent this bill is. Their insight has been essential in putting together our legislation, and I welcome any recommendations they have on how it can be further strengthened.

I also want to state my support for Council Member Rivera's Intro. 1024, which I am proud to co-prime sponsor, and amplify the Coalition's call for legislation that would ban government use of biometric surveillance as well.

I'll know pass it back to Chair Gutiérrez.

CO-CHAIRPERSON GUTIERREZ: Thank you, Council Member Hanif, and I understand that Council Member Rivera has a statement.

CO-CHAIRPERSON WILLIAMS: Sorry. Right before Council Member Rivera goes to do her opening statement on her bill, I just want to acknowledge the Members of the Civil and Human Rights Committee that are here today, Council Members Marte and Richardson Jordan. On to you, Council Member.

COUNCIL MEMBER RIVERA: Thank you so much. Thank you to the Chairs for holding this important oversight hearing and for the opportunity to deliver these opening remarks.

There is a persistent housing crisis in New York City, and, as a former housing organizer and current Council Member, I know that we must use every tool at our disposal to protect tenants and their access to safe and affordable housing. Currently, we are seeing more landlords implementing technological solutions to enhance quality of life and security for residents. But when it comes to facial recognition and biometric identifier systems, there is a gap in the regulatory framework that can lead to negative impacts.

Many New Yorkers share serious concerns when it comes to the use of facial recognition technology and biometrics in different settings, and these concerns are valid and backed by data from common user misidentification to the potential to increase the presence and accuracy of surveillance, and it falls on governments to establish safeguards that protect rights and increase transparency.

Alongside Colleagues and advocates, I have introduced legislation to limit the use of facial recognition technology in residential buildings to ensure New Yorkers do not have their rights violated and are not excluded or discriminated against.

The concerns New Yorkers have about the use of facial recognition technology and biometric identifier systems are real as some have pointed out that this type of technology could further fuel gentrification and even displacement of legacy communities. The Anti-Eviction Mapping Project published a report in 2021 focused on the New York City housing market with narratives from tenants on how facial recognition technology and biometric identifier systems negatively impact their quality of

life and even create a carceral-like environment in the home. Landlords can leverage these technologies to harass tenants by shaking them down for rent and leveling petty lease violations that can lead to eviction. It's a vicious housing market right now with unfettered price raises and displacement. Our city's black population has declined by 200,000 people over the past two decades, and I think about the various factors that lead to the inability of historically marginalized and low-income households to stay here. The rapid expansion of technology is absolutely a pressure that leads to displacement, and it could erode what should be a very diverse collective identity of our city. While technological upgrades can certainly provide a benefit, no doubt, it is our responsibility to ensure that all New Yorkers are protected and that we use technology humanely and appropriately and take into account when it can have negative effects on our civil rights. Housing is a human right, and this legislation seeks to strengthen this.

Thank you very much and, with that, I'll turn it back over to Chair Williams.

CO-CHAIRPERSON WILLIAMS: Thank you. I'd also just like to recognize Council Member Kagan who has joined us from the Technology Committee and Council Member Won from the Technology Committee. Welcome.

COMMITTEE COUNSEL BYHOVSKY: Good afternoon, everyone, and thank you, Council Members for your excellent (INAUDIBLE).

I'm Irene Byhovsky. I'm the Council to the Committee on Technology, and I will be moderating this hearing today.

Now, we move to the testimony from the Administration. Today, we are privileged to have New York City Chief Privacy Officer Michael Fitzpatrick with us to provide his testimony. Additionally, we have Ryan Birchmeier, Deputy Commissioner of Office of Public Safety from the Office of Technology and Innovation and Hillary Scrivani, the Senior Policy Counsel at the New York City Commission on Human Rights to address any questions that might arise during the hearing.

Before we begin, I kindly ask you to raise your right hand. Thank you.

Do you affirm or swear to tell the truth, the whole truth, and nothing but the truth before the Committee today and to respond honestly to Council Member questions?

ADMINISTRATION: (INAUDIBLE)

COMMITTEE COUNSEL BYHOVSKY: Thank you. You may begin your testimony.

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

For those who are unfamiliar with my role, it was established by Local Laws 245 and 247 of 2017, otherwise known as the Identifying Information Law. Implementation of this law began in 2018. Subsequent legislation formally

established the Office of Information Privacy, which I am responsible for leading, and Executive Order 3 of 2022 placed the Office of Information Privacy under the Office of Technology and Innovation as part of the wider consolidation of technology offices. Embedding the Chief Privacy Officer role within the Office of Technology and Innovation has enhanced the consideration of privacy in government operations and initiatives, particularly in matters of technology, by integrating core values such as transparency, data minimization, data integrity, and equity into our agency's work and citywide in close collaboration with our agency partners.

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

it is safe to seek and access assistance and services.

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

Additionally, as the Council is aware, the work of setting citywide privacy policy is supported by the Citywide Privacy Protection Committee. Pursuant to the Identifying Information Law, each agency must biennially report their policies and practices regarding the collection, retention, and disclosure of identifying information to the Mayor, the Speaker of the City Council, and the Chief Privacy Officer. The Citywide Privacy Protection Committee bears the statutory responsibility of reviewing submitted agency reports and developing recommendations for the Chief Privacy Officer relating to policies and

procedures regarding the collection, retention, and disclosure of identifying information.

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

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

community of privacy practice across city government.

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

While biometric identification systems remain an emerging area of technology and privacy practice globally, the framework provided by the Identifying Information Law, along with the steps taken by this administration, have positioned privacy to be duly considered in potential

government utilization of the technology in New York City. We appreciate the opportunity to participate in today's hearing, and, with that, Deputy Commissioner Birchmeier and I will now take Council Members' questions.

CO-CHAIRPERSON GUTIERREZ: Thank you so much and welcome. You're here for the first time. Thank you so much for your testimony.

Can you please describe a little bit more about your role?

CHIEF PRIVACY OFFICER FITZPATRICK: Absolutely. As the Chief Privacy Officer, and as I mentioned in my testimony, I have the responsibility of setting citywide privacy policies and working collaboratively with our network of Agency Privacy Officers that exist across the city. Our office, the Office of Information Privacy, really provides support and advisory services to the agencies, really working collaboratively to create and support an ecosystem of privacy professionals citywide.

CO-CHAIRPERSON GUTIERREZ: Would you also say part of your role is to oversee how agencies use personal information under that purview?

CHIEF PRIVACY OFFICER FITZPATRICK: I would say that part of my role is to facilitate the setting of citywide policy that agencies are obligated to follow pursuant to the Identifying Information Law and supporting the Agency Privacy Officers in implementing those policies. The Identifying Information Law really creates in support of that ecosystem of self-governance an empowerment at the agency level of making and evaluating the determinations about their privacy practices and policies through the lens of both lawfulness and the lens of the agency's unique mission and purpose.

CO-CHAIRPERSON GUTIERREZ: With respect to every agency's individual protocol, your team is also overseeing how that is executed?

CHIEF PRIVACY OFFICER FITZPATRICK: We are provided information pursuant to the Identifying Information Law on agency privacy practices and policies that occurs in a number of different ways. There's the biennial reporting that occurs that's provided to my office. Additionally, we receive regular reporting from agencies in the event that identifying information has been disclosed or collected in a manner that violates Local Law and

contemporaneously provide periodic reporting to the Speaker of the Council on those circumstances.

CO-CHAIRPERSON GUTIERREZ: Thank you. The Identifying Information Law, Local Laws 245, 247 of 2017, sets forth requirements for city agencies to follow in the event that agency collection and/or disclosure of personally identifiable information constitutes a breach of security. There is a form for New Yorkers to file a complaint in that event that personally identifiable information has been collected or disclosed in a manner inconsistent with the requirements of the Identifying Information Law. Can you share how many complaints you have received and/or how many this year?

CHIEF PRIVACY OFFICER FITZPATRICK: I've been in the role as Chief Privacy Officer for a little over a year now. Over that time period, we have received one complaint, and, historically, my office I think we have, the unofficial number or the best number that we have available is less than 10.

CO-CHAIRPERSON GUTIERREZ: Less than 10?

CHIEF PRIVACY OFFICER FITZPATRICK: Yes.

CO-CHAIRPERSON GUTIERREZ: Okay, and how do you make New Yorkers that this complaint form exists?

CHIEF PRIVACY OFFICER FITZPATRICK: Sure. As part of our consolidation within the Office of Technology and Innovation, which is really the hub of technology services now citywide, we can be engaged through the Contact the Leadership Team of the Office of Technology and Innovation page on our website.

CO-CHAIRPERSON GUTIERREZ: Got it. Is OTI considering any regulations under the Identifying Information Law that would address potential disclosure of biometric information?

CHIEF PRIVACY OFFICER FITZPATRICK: That's a great question, Council Member, and it's really the area of emerging technology that really was a motivation of changing the Citywide Privacy Protection Committee's cadence to allow us to be more engaged and in collaboration as a privacy community to discuss these areas of emerging technology.

CO-CHAIRPERSON GUTIERREZ: So it's something that you're kind of exploring at this…

CHIEF PRIVACY OFFICER FITZPATRICK: Absolutely.

CO-CHAIRPERSON GUTIERREZ: Okay. Do you have any examples or instances where biometric data was disclosed?

CHIEF PRIVACY OFFICER FITZPATRICK: Can you be more specific on that?

CO-CHAIRPERSON GUTIERREZ: Just in following up to the previous question about amendments or changes to the Identifying Information Law. The question was about disclosure of biometric information, and you're saying it's evolving and you're kind of like adjusting. Do you have any examples of that happening to date?

CHIEF PRIVACY OFFICER FITZPATRICK: Sure, absolutely. Thank you, Council Member, for the clarification.

As part of that quarterly reporting that I mentioned earlier that's provided to the Council on instances where citywide we've had identifying information disclosed in a manner that violates Local Law, that would be inclusive of any instances where biometric data elements were disclosed. I think it's also important to note in that context there's a distinction between biometric data elements and

utilization of those elements in connection with an identification system for example.

CO-CHAIRPERSON GUTIERREZ: Thank you. Pursuant to Administrative Code Title 23 Section 1205, each agency must submit identifying information reports. The reports include information on the type of data collected by each agency. Can you tell us what agencies collect biometrics?

CHIEF PRIVACY OFFICER FITZPATRICK: It depends on the data elements. We have enumerated data elements that would fall into the biometric category. An example was provided directly in the Identifying Information Law's photographs so, unsurprisingly, there's a large number of agencies that identify the collection of photographs. An example use case in that circumstance would be for issuing, for example, employee identification cards. That would have to be identified as a collection at the agency level but does not necessarily indicate a use of those photographs in furtherance of a biometric identification system. We actively, and it's an area where I'm happy to share with the Committee the investments that this Administration is making in further developing the capabilities and resources of

our office. Current state, we are a team of six folks, and the Administration, and we're grateful for their support, we are actively working to more than double our office in the near-term. We're moving from a staff of exclusively attorney membership to include non-attorney roles, specifically inclusive of onboarding privacy analysts who will support our work in further refining our reporting mechanisms and policies, supporting the developments of key metrics and allowing for us to get better visibility about what we are seeing citywide in the space of identifying information inclusive of biometric data elements.

CO-CHAIRPERSON GUTIERREZ: Any agencies that use fingerprints to collect biometrics that you can share as agencies that are providing reports or collecting data to you all?

CHIEF PRIVACY OFFICER FITZPATRICK: Absolutely. I don't have that information in front of me, but I'm happy to provide that information to the Committees.

CO-CHAIRPERSON GUTIERREZ: Can you at least me know, I'm just going to ask specific agencies, if you can confirm with me whether or not

they collect biometric data? The first one is DHS, do they fingerprint in our shelters?

CHIEF PRIVACY OFFICER FITZPATRICK: I would need to confirm the agency report.

CO-CHAIRPERSON GUTIERREZ: Okay. Same agency, you don't know if they use facial recognition or other biometric data?

CHIEF PRIVACY OFFICER FITZPATRICK: Not that I'm aware of.

CO-CHAIRPERSON GUTIERREZ: Okay. Are you aware if ACS uses biometric data?

CHIEF PRIVACY OFFICER FITZPATRICK: Not that I'm aware of.

CO-CHAIRPERSON GUTIERREZ: No? Okay. What about NYCHA?

CHIEF PRIVACY OFFICER FITZPATRICK: Sorry. For ACS, I want to clarify biometric identification systems I'm not aware of. I can specify the data elements that they're collecting and follow up to the Committee.

CO-CHAIRPERSON GUTIERREZ: You want to follow up with that? You don't have it right now?

CHIEF PRIVACY OFFICER FITZPATRICK: Yes.

CO-CHAIRPERSON GUTIERREZ: Okay. Because a followup question would be what decisions are being made using this data.

What about Public Housing?

CHIEF PRIVACY OFFICER FITZPATRICK: Public Housing, Public Housing if we're referring to NYCHA, NYCHA is an entity that is not subject to the Identifying Information Law by virtue of its regulatory structure so I don't have the same degree of visibility that I would at other agencies, but I can say that I'm now aware of any sort of biometric identification system.

CO-CHAIRPERSON GUTIERREZ: What about with the Department of Education?

CHIEF PRIVACY OFFICER FITZPATRICK: Actually same answer there. Also not subject to the Identifying Information Law by virtue of their regulatory structure, but I'm also not aware of any use of biometric identification systems.

CO-CHAIRPERSON GUTIERREZ: Thank you. Lastly in this section, are you aware if LinkNYC uses facial recognition or other biometric technology?

CHIEF PRIVACY OFFICER FITZPATRICK: My understanding is that LinkNYC does not use facial recognition technology.

CO-CHAIRPERSON GUTIERREZ: Okay. Lastly, is the City collecting any data from private partners or private entities?

CHIEF PRIVACY OFFICER FITZPATRICK: Can you be more specific, Council Member, on any…

CO-CHAIRPERSON GUTIERREZ: Yeah. I don't mean to like lean into the MSGPs but any private institution that is collecting data, are you holding them accountable or connecting with them on the data that they are collecting.

CHIEF PRIVACY OFFICER FITZPATRICK: Sure, absolutely. Thank you for the clarification, Council Member. For that mechanic to take place, and that's really a reflection of the ecosystem of self-governance that I've been referencing, those are determinations that are made at the agency level in accordance with the Identifying Information Law and associated policies so, for example, if an agency were endeavoring to collect information from a private entity, for example, that collection would need to be reviewed by the agency privacy officer who

would evaluate it through that lens of lawfulness and mission and purpose of the agency as well as citywide privacy policy before the collection could occur.

CO-CHAIRPERSON GUTIERREZ: I see. Can you share of any of those instances where agencies are doing that from private entities?

CHIEF PRIVACY OFFICER FITZPATRICK: Not at this time.

CO-CHAIRPERSON GUTIERREZ: Okay. My next question is regarding just data security. For city agency biometric systems that OTI has approved or oversight over, for example, NYPD's facial recognition services, are these systems using Cloud infrastructure to collect and store biometric data or is the data collected and stored in a local processing unit?

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you for the question, Council Member. That's a circumstances that's really going to be dependent on an agency use case by use case…

CO-CHAIRPERSON GUTIERREZ: But PD specifically.

CHIEF PRIVACY OFFICER FITZPATRICK: For example, if we were talking about the utilization of

Cloud resources, for example, that would be a touchpoint that exists that's required to go through a Cloud security review conducted by the Office of Cybercommand to ensure the security of the ecosystem before it's utilized, and that's any Cloud service that's utilized.

CO-CHAIRPERSON GUTIERREZ: Sure. I can understand that, but can you confirm whether or not PD is using a Cloud storage system for data storage?

CHIEF PRIVACY OFFICER FITZPATRICK: I cannot. I'd have to refer you to the NYPD on the specific deployment of its technology.

CO-CHAIRPERSON GUTIERREZ: Well, we tried to get them here today.

In other instances, but can you confirm if other agencies, maybe you can't name them all, but can you confirm if other agencies are utilizing Cloud infrastructure to store data?

CHIEF PRIVACY OFFICER FITZPATRICK: I can confirm that other agencies are using Cloud resources for data storage generally.

CO-CHAIRPERSON GUTIERREZ: Perfect, thank you. Do you have a sense, can you share who controls access to the data?

CHIEF PRIVACY OFFICER FITZPATRICK: That's a great question, Council Member. From a privacy perspective, it's an area that really hinges on not just our privacy policies but the associated contracting guidance that we provide agencies so when we look at these particular vendor engagements, we're not only looking at them through the lens that I mentioned earlier about APO involvement and approval and assessment and approval or denial, but we're looking at it through the lens of contracting to make sure that we've got appropriate terms attached to ensure that the City not only has visibility into what's happening on the vendors' side in making sure that they've got appropriate safeguards from a security perspective but means of holding the vendors accountable in the event that there has been a compromise in some way.

CO-CHAIRPERSON GUTIERREZ: Is your team helping to set the terms with that vendor with respect to each agency?

CHIEF PRIVACY OFFICER FITZPATRICK: We provide standard terms that we've developed collaboratively with the Law Department, and the default is that these are the terms and they shall

not be changed unless and until there's a consultation with the Chief Privacy Officer.

CO-CHAIRPERSON GUTIERREZ: That is you?

CHIEF PRIVACY OFFICER FITZPATRICK: That is me.

CO-CHAIRPERSON GUTIERREZ: Okay. I'm sorry if you answered this already but, per those terms, who owns the data?

CHIEF PRIVACY OFFICER FITZPATRICK: It's going to be dependent on the circumstance, but we would say that it's City data.

CO-CHAIRPERSON GUTIERREZ: Okay. Could say that your agency owns the data?

CHIEF PRIVACY OFFICER FITZPATRICK: It would be dependent on the circumstance. If, for example, if we are in a facilitation role of building a conduit between two different agencies, those agencies would be the data custodian and we would just be enabling them from a technology perspective.

CO-CHAIRPERSON GUTIERREZ: Okay. Would you say that that also applies to biometric identification captured by PD?

CHIEF PRIVACY OFFICER FITZPATRICK: I would have to look into that further on the specific role of OTI and any utilization of that technology.

CO-CHAIRPERSON GUTIERREZ: Okay. That would be helpful if they're being held to the same standard as all the other agencies are.

CHIEF PRIVACY OFFICER FITZPATRICK: I can say certainly that the PD, like all other agencies that are subject to the Identifying Information Law, are subject to the associated policies and the utilization of the contracting terms that I've mentioned.

CO-CHAIRPERSON GUTIERREZ: Fantastic. Thank you. My next question is regarding IDNYC. When you first go to apply for IDNYC obviously they are voluntarily sharing biometric data as well as a photograph. Can you just confirm who has access to the applicant's personal information and if that's shared with any other agencies?

CHIEF PRIVACY OFFICER FITZPATRICK: I would say that the operating agency would be best positioned to speak to those particular mechanics, Council Member, but, generally speaking, those collections as I understand them are occurring for

the purpose of enrolling particular applicants in programs that they may be eligible for so those collections are being evaluated by the agency privacy officer in accordance with the Identifying Information Law, and any disclosures that would be necessary would also have to be equally evaluated through that lens inclusive of other government entities, even at the federal level.

CO-CHAIRPERSON GUTIERREZ: I understand. I also just want to acknowledge Council Member Rita Joseph and Council Member Gale Brewer who have joined us.

My next series of questions are regarding DigiDog and K5 ASR. I know some of my Colleagues may have some of these questions as well. I just want to confirm a couple of things. DigiDog and K5 ASR, they have camEras, correct?

CHIEF PRIVACY OFFICER FITZPATRICK: My understanding is that they do.

CO-CHAIRPERSON GUTIERREZ: They do? Okay. Can you share what data they collect?

CHIEF PRIVACY OFFICER FITZPATRICK: My understanding, and, again, I would refer you to PD for the specific capabilities, but my understanding

for K5, for example, is that there is video data collected and the capability of recording audio data if a particular button is pushed on the device by an individual looking to make a report, for example.

CO-CHAIRPERSON GUTIERREZ: All right. What about DigiDog?

CHIEF PRIVACY OFFICER FITZPATRICK: I believe there's a video capability with DigiDog. Less certain about the audio component, but the deployment postures for each of those technologies as I understand them, there's a pilot for the K5 that's contemplated within the Times Square subway station. That was publicly announced by the Mayor and NYPD leadership and DigiDog, the utilization of that technology is reserved for specific emergency response scenarios where, for example, it would be dangerous for a human member of the service to enter a premises.

CO-CHAIRPERSON GUTIERREZ: Okay. Do you know if DigiDog or K5, if they're able to recognize faces live?

CHIEF PRIVACY OFFICER FITZPATRICK: My understanding is that they cannot.

CO-CHAIRPERSON GUTIERREZ: Okay. Do you know if any of the data, audio, video that both DigiDog and K5 capture, do you know if any of that footage can be used to later identify individuals?

CHIEF PRIVACY OFFICER FITZPATRICK: I would make the distinction there that while the conduit of the technology is a robotic device, the associated technology attached to it is really the function of any other video camera so there certainly could be the capability that in response to and as part of a criminal investigation, a still image captured from one of those devices could be utilized for facial recognition technology purposes by the Police Department.

CO-CHAIRPERSON GUTIERREZ: Okay. I understand that. I think would love to dig in deeper at a later time because I know what, certainly the makers of DigiDog are saying is that it doesn't recognize faces and I get that, but I think the association of using any footage to later identify is also problematic and so I think what's being told to New Yorkers is not fully sincere around what these DigiDogs are capable of in the long-run in potentially identifying and targeting New Yorkers.

CHIEF PRIVACY OFFICER FITZPATRICK: Absolutely, Council Member, and I completely understand the concern there, and I think it's an important illustration of the conversation that we're having today that we can provide that clarification as well as the steps that the Mayor and NYPD leadership took to publicly announce the capabilities of those technologies at I think at least a handful of settings at this point.

CO-CHAIRPERSON GUTIERREZ: Do you support the use of facial recognition and other biometric technologies in the city?

DEPUTY COMMISSIONER BIRCHMEIER: I would just say yes, OTI absolutely does not and it's not specific to facial recognition technology but certainly any emerging technology that an agency feels will be beneficial to their operation but is deployed in a lawful and responsible way.

CO-CHAIRPERSON GUTIERREZ: Do you support the use of FRT by private companies?

DEPUTY COMMISSIONER BIRCHMEIER: Private companies, because OTI has so little dealing with the private sector, we are an internal-facing organization, we support government agencies doing

that. We don't feel like we are the right body to be commenting on how a private business is operating.

CO-CHAIRPERSON GUTIERREZ: Is there a body that you believe is more equipped to do that for the private industry?

DEPUTY COMMISSIONER BIRCHMEIER: I don't know. I'd have to refer you to the Mayor's Office I guess for…

CO-CHAIRPERSON GUTIERREZ: I think it does. I think it is something that OTI should…

DEPUTY COMMISSIONER BIRCHMEIER: Yeah, I think that specific issue has so many stakeholders involved that we are not regularly speaking with and so for that reason I don't feel like we're the best folks to comment on the private business' operations.

CO-CHAIRPERSON GUTIERREZ: But there is concern here at this Council for the way that private industries are using facial recognition technology or biometric data to serve their very rich and robust business model at the expense of marginalized New Yorkers, and that is my recommendation is that maybe working together, but I don't think that that's something that we can just say bluntly, well, there's

too many stakeholders, we can't really take this on. I don't think that's fair.

DEPUTY COMMISSIONER BIRCHMEIER: Yeah. Absolutely noted and completely understand the concern.

CO-CHAIRPERSON GUTIERREZ: Can you share if the City has ever requested or obtained biometric data from private companies or landlords that are doing collection in New York City including NYCHA?

DEPUTY COMMISSIONER BIRCHMEIER: Not that we're aware of.

CO-CHAIRPERSON GUTIERREZ: Do you know if any agencies purchase or sell data to and from data brokers?

DEPUTY COMMISSIONER BIRCHMEIER: Not that we're aware of.

CHIEF PRIVACY OFFICER FITZPATRICK: No, not that we're aware of, and just to supplement that point, Council Member, that's really another illustration of how the Identifying Information Law is operationalized. We look at it through the lens of lawfulness, we look at it through the lens of mission and purpose, but we also look at it through the lens of our privacy principles inclusive of which are

considerations of use specification, data minimization, and, frankly, equity. Equity was a principle that we actually just recently added in our updated policies earlier this year, recognizing that as we're enabling and building our privacy culture within city government operations and as we're thinking through these issues, we necessarily should be sensitive to the fact that as a government entity we are custodians of some information for some universes of folks more than others and calibrate those decisions accordingly.

CO-CHAIRPERSON GUTIERREZ: Thank you. I just have a couple more questions before I pass it off to Council Member Williams. Thank you for your patient, Nan.

Can you share what facial recognition technology the NYPD uses?

CHIEF PRIVACY OFFICER FITZPATRICK: NYPD's use of facial recognition technology is detailed in the City's annual reporting of algorithmic tools, and so I believe the company that they list in the annual report is DataWorks.

CO-CHAIRPERSON GUTIERREZ: DataWorks. I'm really glad that you brought up incorporating equity

into your principles. As you know, a lot of concern in our communities are related to using the marriage of facial recognition technology and other collections of biometric data to target and harm people of color, men and women of color. Do you have a sense of how can we ensure the technology that NYPD uses, for example, accounts for racial bias?

DEPUTY COMMISSIONER BIRCHMEIER: I think it's an absolutely valid concern that every city around the country and world is dealing with and every body of government is dealing with this. We think of this in a number of ways, and I think from the Administration standpoint we've developed an ecosystem of governance to help ensure that every stakeholder is accounted for along the way when technology is developed. I think the citywide privacy policy is absolutely one of those elements to see how data is being used. I think citywide cybersecurity policy to see how data is being stored, Local Law 35 which requires transparent use of any algorithmic tool is certainly one, the Human Rights Law to make sure that any violation of human rights is held accountable. We also use the National Institute of Standards and Technology's framework to assess tools

and their risk for discrimination, but further the Administration and OTI is leading this effort is developing an AI action plan that will develop a governance for how agencies are evaluating testing and piloting if they deem it appropriate any algorithmic based tool which would include facial recognition technology and risk for discrimination is going to be a critical part of that.

CO-CHAIRPERSON GUTIERREZ: Who provides oversight over PD to ensure that they're doing all these things that you're saying, that they are complying with their own facial recognition policy and that it's only being used for "legitimate" le purposes? I think that's the piece that with the release of DigiDog and K5, obviously there's a lot of information that is being released and we're all kind of learning at the same time, but I think that there's a big and valid concern in our communities about who is doing the oversight for PD. I mean historically they've been able to launch programs and initiatives for months before they even announce it to New Yorkers and so oftentimes we are vulnerable, oftentimes New Yorkers have no sense of whether their information is getting collected. Oftentimes, New

Yorkers don't even know their information is sitting in a database, i.e., the gang database, so who is doing that oversight of PD to ensure that they're following a protocol that you are saying exists, and I believe it and that every agency is being held to, but who is doing that for PD?

DEPUTY COMMISSIONER BIRCHMEIER: I would say that everything that I just listed, the New York City Human Rights Law, we oversee, and NYPD like every other agency across the City government has been in compliance with all of the governance that I allowed.

CO-CHAIRPERSON GUTIERREZ: I just don't believe that, but I will read any and all reports that you send me.

CHIEF PRIVACY OFFICER FITZPATRICK: To supplement Deputy Commissioner Birchmeier's information, I think it's important too when we're looking at the issue of potential for discrimination, we have to acknowledge that the risk exists. Within the last week or so, we saw a joint statement at the federal level by a number of agencies affirming the position of the federal government against discrimination, acknowledging the risk posed by AI

and automatic decision systems but recognizing while these technologies may be new they are nonetheless subject to the existing regulatory authorities of entities at the federal level, and certainly I don't think that would be any different locally, right. As we're having this conversation today, we're showing how biometric technology is considered through the existing regulatory scheme of the Identifying Information Law. When we're talking about potential oversight, we're talking about touchpoints, and Deputy Commissioner Birchmeier identified several of them. Additionally, I think it's important to note when we're thinking about the Police Department's use case, for example, we've also not only be operating in a universe where I think there's been a tremendous amount of transparency particularly under this Administration about what the Police Department is doing and why, but additionally that the utilization of facial recognition technology, for example, is also occurring in an environment where, since 2020, there has been an expanded universe of criminal discovery in prosecutions so to the extent that the technology is utilized, that information is available to the Defense Bar, for example, which would in turn

have the capability of challenging the use of the technology in the context of prosecution but certainly informing the basis of subsequent civil litigation that may follow as appropriate.

CO-CHAIRPERSON GUTIERREZ: Thank you. How can New Yorkers learn about which private home surveillance footage is used in police investigations and are they required to report this usage besides New Yorkers having to request a FOIA, for example?

CHIEF PRIVACY OFFICER FITZPATRICK: Sorry, could you be more specific (INAUDIBLE)

CO-CHAIRPERSON GUTIERREZ: Sure. I guess the angle of the question is how to inform more New Yorkers about how to be empowered to learn whether they're on some kind of a list or if their information is being captured by PD and so how can New Yorkers learn about which of that footage, for example, is being used in police investigations for their own private home surveillance?

CHIEF PRIVACY OFFICER FITZPATRICK: Sure. From a privacy profession perspective, we're talking about the conversation, the term of art typically used is data subject rights for privacy frameworks globally, largely in the private sector. When we're

talking about government operations, the term of art is typically in the Freedom of Information context, either at the federal level or the local level, and that would be the best mechanism, I think, for New Yorkers to request information about themselves that may be held by any agency.

CO-CHAIRPERSON GUTIERREZ: What is the best way? I apologize.

CHIEF PRIVACY OFFICER FITZPATRICK: Freedom of Information.

CO-CHAIRPERSON GUTIERREZ: Oh, so the only option right now is a FOIA request? Okay.

My last question before passing it off to Council Member Williams is regarding MyCity portal you all launched now two months ago, congrats. Does the Administration have any plans to incorporate biometric data or other identification technologies into the MyCity portal.

DEPUTY COMMISSIONER BIRCHMEIER: Not at this time.

CO-CHAIRPERSON GUTIERREZ: Thank you. Council Member and Chair Williams.

CO-CHAIRPERSON WILLIAMS: Thank you. Can you just share, again, like your oversight functions

of other city agencies to ensure that they're maintaining privacy? What is your actual function?

CHIEF PRIVACY OFFICER FITZPATRICK: Sure. Thank you for the question, Council Member. I would not necessarily characterize our role as oversight. We are really a partner among that citywide ecosystem of privacy protection in advancing privacy practices at the agency level. We effect that regular engagement with our Agency Privacy Officers, support them when they reach out to us with questions, engage them when we become aware of matters of concern at their agency, and additionally facilitate reporting from the agencies in the event that identifying information is disclosed in a manner that violates Local Law, facilitate the preparation and reporting of that information to the Council on a quarterly basis. An illustration of why I'm hesitant to use the term oversight. Purposefully within the Identifying Information Law, that reporting de-identifies specific agencies from being named in the reporting that's shared with the Council. I think that was done purposefully so because we want to make sure that agencies feel comfortable engaging our office and not that they would necessarily be negatively shamed for

instances where identifying information has been disclosed in a manner that violates Local Law.

CO-CHAIRPERSON WILLIAMS: I am so happy you mentioned the Identifying Information Report because I have a question on that because we do observe that your office provides no details, it doesn't have the agency, it doesn't list out exactly what the disclosed information was, and it provides only a short sentence of what the remedy is so do you think your office has been effective since it seems like a pretty collegial relationship and not one that can truly hold an agency accountable if they're in violation?

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you for the comment, Council Member. I would say that the work of our office has really been one of leadership in the privacy field since it was created a little bit more than five years ago. I think the work that the team has done in developing this privacy governance framework on a citywide level, particularly when that city is New York City, has been truly remarkable, again factoring in that we're historically a team of about five or six folks, but I think that what's reflected in those reports is not

necessarily a reflection of the depth and detail and conversations that are happening among my staff and the agencies about what is specifically occurring at the agency level and supporting the agency remediation of concerns, but I'm appreciative certainly of the feedback that you're providing, Council Member, and will certainly bring that back to the team, and we'll consider it moving forward for future reporting.

CO-CHAIRPERSON WILLIAMS: Yes. It's hard to assess whether or not agencies are properly remediating issues if, for instance, we can't tell like the last quarter had 30 violations. For all we know, it could've been the same agency that had those 30 violations, but there's no way for us to even hold a particular agency accountable for a particular violation because your office provides no details.

CHIEF PRIVACY OFFICER FITZPATRICK: I appreciate that, Council Member, as well. I will point out that the lack of identification of agencies in that particular report is done purposely pursuant to the Identifying Information Law though I will certainly say that is an area that I'm actively looking into. That is an area that is one of many

reasons why we are bringing on an analyst capability within our office to support a better understanding of what we are seeing at a citywide level in furtherance of also developing key performance metrics, etc. from a privacy perspective.

CO-CHAIRPERSON WILLIAMS: Do you have any recommendations on how that law can be strengthened since its creation?

CHIEF PRIVACY OFFICER FITZPATRICK: From my perspective, I think the Law has been operationalized I think quite effectively and I think in a very thoughtful way positions the Chief Privacy Officer to be the steward of setting that citywide privacy regulation at intervals that the cop determines are necessary and certainly in response to areas where technology policy needs to be evolved or revised in some way in response to developments.

CO-CHAIRPERSON WILLIAMS: Okay. Two more questions for you. During a previous hearing, your colleague, the Chief Tech Officer, testified about a project to label all public eye technology equipment including surveillance equipment to inform the public about their functions. Does the current

Administration support such an initiative and, if so, when can we expect the project to roll out?

DEPUTY COMMISSIONER BIRCHMEIER: Do you have any more context on that project?

CO-CHAIRPERSON WILLIAMS: I can get you more context, but apparently it was a project…

DEPUTY COMMISSIONER BIRCHMEIER: I didn't hear the beginning of the question…

CO-CHAIRPERSON WILLIAMS: Oh. It was a project to label all public eye technology equipment including surveillance equipment to inform the public about its function so the Administration was supposed to create a list and then the list was supposed to be released to give the public an idea of all the different types of technologies that are being used.

DEPUTY COMMISSIONER BIRCHMEIER: Yeah, I'm happy to check with the Chief Technology Officer on the status of that project and circle back with your office.

CO-CHAIRPERSON WILLIAMS: Okay, yeah, it's something that he said at a previous hearing so we're just trying to figure out…

DEPUTY COMMISSIONER BIRCHMEIER: Yeah, of course, I'm happy to look into it more and circle back to you.

CO-CHAIRPERSON WILLIAMS: Okay. There are some Members that have to leave in a second so I will stop to be so kind to my Colleagues starting with Council Member Joseph.

COUNCIL MEMBER JOSEPH: I get to go first?

CO-CHAIRPERSON WILLIAMS: Yes, you're first.

COUNCIL MEMBER JOSEPH: Thank you. My questions were around what privacy concerns have been raised by the use of biometric identification systems and how has the City addressed them?

CHIEF PRIVACY OFFICER FITZPATRICK: Sure. Thank you for the question, Council Member. The chief concern that we certainly see from being really students of the privacy profession globally is the risk of discriminatory impacts, and, in response to those risks, I think we certainly look to the revisions to our privacy policies earlier this year which added equity as a privacy principle for agencies to consider when evaluating privacy concerns, the steps that the Administration has taken

to reimagine the citywide Privacy Protection Committee to be engaged in a more regular manner on these types of emerging technology issues, and, as Deputy Commissioner Birchmeier mentioned earlier, stewarding the development of not only an artificial intelligence action plan to help guide lawful and responsible use of these technologies citywide but also actively hiring for a Director of Artificial Intelligence and Machine Learning to be responsible directly for this portfolio.

COUNCIL MEMBER JOSEPH: Thank you for that. What kind of data security measures are in place to protect biometric data collected by these systems and how is access to this data restricted?

CHIEF PRIVACY OFFICER FITZPATRICK: Absolutely. Thank you for the question, Council Member. From a privacy perspective, we look at it through the lens of ensuring that there's data minimization as a principle, that the folks who have access to that information have a justifiable need for that access, and then from a technical perspective rely on and work in partnership with the Office of Cyber Command in making sure that there are sufficient technical controls and security controls

in place that are in accordance with citywide cyber security policy.

COUNCIL MEMBER JOSEPH: In terms of application, what type of application? You mentioned AI. Are you using AI into how you gather data?

DEPUTY COMMISSIONER BIRCHMEIER: I would just say one of the reasons we feel like there needs to be an actual centralized AI framework is in it's in so many things including our personal gmail that reminds you to respond to an email to a friend so it's baked into so many things that it can no longer be treated as that's an AI tool. It's kind of foundational in a lot of things, and so that's why we want to have a centralized framework so that any tool that has that baked in, folks can go through a governance process to check everything from security to privacy to risk for discrimination and to see if it's an appropriate use for their agency.

COUNCIL MEMBER JOSEPH: Thank you so much. Thank you, Chairs.

CO-CHAIRPERSON WILLIAMS: Your welcome. Next, Council Member Rivera.

COUNCIL MEMBER RIVERA: Thank you so much for the time. I will be brief, and I want to thank

you all for your testimony. I want to thank everyone who's here including the advocates who helped write this bill.

You mentioned a few of the agencies that you said that you're not aware of if they use the data or how they use it, but also in your testimony you included the law that you feel has created a framework that I think you describe as appropriate. However, I want to ask do city agencies track the usage of biometric identification systems in residential settings? Does OTI or other city agencies have any data to share that indicates trends in building owner usage of residential biometric identification systems and what is your approach? Do you support the legislation that we're hearing today?

DEPUTY COMMISSIONER BIRCHMEIER: Thank you, Council Member, for your question and for your testimony earlier. I'm not aware if any city agencies are tracking biometric technology use across residential buildings. I'm happy to check with my Colleagues who work at HPD or NYCHA and circle back with you and provide you with that. On the specific legislation, because OTI is not squarely in the housing space and we're not having regular

conversations with tenants, tenants' advocates, or landlords, we don't feel like we are the best people to speak to the bill, though obviously the nature of the bill is a conversation we're happy to be having with you today.

COUNCIL MEMBER RIVERA: Understood, but you do describe in your testimony that you are here to integrate core values of transparency and data integrity and you work in close collaboration with citywide agency partners so that's why we're asking you these questions. How does the City support building owners who are interested in pursuing biometric identification systems for their properties? How does your Department ensure that New York City tenants are aware of Local Law requirements and their privacy rights?

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you for the question, Council Member. Our office currently has a role pursuant to the Operative Private Sector Biometrics Law and working collaboratively with other city agencies and conducting outreach to entities about what the Law requires. We've effected that outreach through the development of a FAQ that's posted publicly available

on our website as well as DCWP's website. We're an office that, as I think we've been discussing today, our mission and primary area of concern is really internal to government operations. We have had a limited number of engagements and inquiries from the private sector about what the Law requires. In that setting, obviously, we're not counsel to those entities. We effectively direct them to the FAQ and really advise them that they need to consult with their own attorneys before the implementation of those technologies.

COUNCIL MEMBER RIVERA: So there's an FAQ? I look forward to your check-in with HPD to see how we can further discuss implementing this legislation and gaining the Administration's support.

For the FAQ, that's a good start, but this is certainly something that's here to stay, and so there has to be continued collaboration across the board.

DEPUTY COMMISSIONER BIRCHMEIER: Absolutely.

COUNCIL MEMBER RIVERA: Thank you. Thank you to the Chairs for the time.

COUNCIL MEMBER BREWER: Thank you. My question is a little bit of followup. On the (INAUDIBLE) keys which NYCHA residents have, mostly I think in buildings that are being privately managed, the residents hate them. Is that something that you keep tabs on? Is there any data that is collected from that? I don't know.

DEPUTY COMMISSIONER BIRCHMEIER: I'd have to refer to NYCHA on that question.

COUNCIL MEMBER BREWER: Okay, but you're in charge of technology for the City though.

DEPUTY COMMISSIONER BIRCHMEIER: Yes.

COUNCIL MEMBER BREWER: So you wouldn't have any idea?

DEPUTY COMMISSIONER BIRCHMEIER: No, and I think in our role more broadly, like I said earlier, we are setting governance structures, we're helping agencies make technology decisions but, operationally, these agencies are empowered to make decisions on a day-to-day basis that effect their day-to-day business and so that specific instance, I think I'd have to refer to NYCHA, and our office is happy to get that answer for you and get…

COUNCIL MEMBER BREWER: Okay. The second question is relevant to just storage. I know quite a bit about technology. How, where, cost, etc. Just generally the data that you do have that is under your control, where do you store it, what's the cost factor, how long does it last, etc., and, if there is a mixing of public and private which could happen, how does that work, storage in general.

DEPUTY COMMISSIONER BIRCHMEIER: Storage is obviously a…

COUNCIL MEMBER BREWER: It's a big topic (INAUDIBLE) I understand that.

DEPUTY COMMISSIONER BIRCHMEIER: I don't have any specific numbers in terms of budgetary factors, but I can say that any private company that is storing data, we certainly store a lot of it in-house. Certainly, if we have any private partners that are storing data, they have to go through very strict privacy security protocols and other vendor protocols to even make it onto the list and make sure that they are adhering to our standards. Happy to get you a better snapshot of what that looks like though after the hearing.

COUNCIL MEMBER BREWER: I'd love to know where, how much, and the relationship between public and private, yes. Thank you very much.

CO-CHAIRPERSON WILLIAMS: Council Member Sanchez, did you want to provide some remarks?

COUNCIL MEMBER SANCHEZ: Thank you so much, Chairs. Yes, I would. Thank you. I was just coming out of the Housing and Building hearing.

I just want to join in my Colleagues remarks and reiterating that we firmly believe in the right to privacy and protection against discrimination, and that is what these bills are intending to address. We've seen time and again that the use of biometric technology and particularly facial recognition technology is subject to algorithmic bias, and this can result in the excess and unfair targeting of nonwhite men, people of color, women, trans women, immigrants, transgender individuals. We want to make sure that there is absolutely every single safeguard is being put in place that's within our power to regulate as a City, right.

Particularly as Chair of the Committee on Housing and Buildings, I'm proud to co-prime Intro.

1024 with Council Member Rivera, which would make it unlawful, you know what the bill does, to install activator use biometric recognition technology. Being mindful of the time, I would be interested to know firstly how your Office collaborates with the privacy officer at HPD and what their role is in protecting tenants in particular and your position on the bill, does the Administration have any hesitation on restricting landlords' ability to use biometric technology in residential buildings? Thank you, Chairs.

DEPUTY COMMISSIONER BIRCHMEIER: Of course, I'll answer the second part of your question and I'll kick it over to the Chief Privacy Officer. Just on the position of the bill, like I said to Council Member Rivera, OTI, just because we are not specifically in discussions with tenants, tenants' advocates, landlords, we are not in a position to take a stance on the bill. The Mayor's Office would be happy to get you the Administration's stance on that bill, but, that said, I think the CPO can talk about their relationship with HPD.

CHIEF PRIVACY OFFICER FITZPATRICK: Absolutely, thank you. Thank you for the question,

Council Member. I think what's really important in HPD and really all of our Privacy Officers, and it's truly, I would characterize it as a remarkable result of the Identifying Information Law, what we actually have here in New York City is a network of privacy professionals that not only are sensitive to the work inherent within that profession but they carry the expertise through the lens of their agency's unique mission purpose and regulatory scheme, and we have the capability of engaging with any one of them as do they directly with our office, HPD included. We've also, since I've been in the CPO role, have done some additional steps. We are accessible, we do have open door policies, but there's also standing time reserved on my calendar every week that any agency privacy officer can claim and set a meeting with me whenever they feel the need to.

COUNCIL MEMBER SANCHEZ: Thank you. Chairs, if you would allow me. It's a little odd to hear you say that you are not taking a position but the Admin will. When you come to one of our hearings, you are representing the Administration so look forward to seeing the Administration's position on

these bills and having that be the case moving forward. Thank you.

CO-CHAIRPERSON WILLIAMS: Thank you. I don't have any more questions for you. I have questions for CCHR so I'm going to turn to my Colleagues who have questions for you so Council Member Holden.

COUNCIL MEMBER HOLDEN: Thank you. Thank you, Chairs. I'm a little surprised that we don't have the Administration's stance also on these bills. That's why we're here. Otherwise, we're spinning our wheels a little bit.

I have some questions because I just see these two bills as a little overreach on businesses. When government gets involved in prohibiting certain investments that a business made to protect themselves and they bought the service or that a landlord decides I have to protect my renters or my owners because they're getting maybe certain burglaries or certain other things happening to their building so they're doing what legally they can do, and now all of a sudden the rug is pulled out. For instance, Madison Square Garden has used the technology to keep people who have committed violence

out of their arena so I'm concerned, and maybe you can weigh on this, are you concerned that by banning this technology, facial recognition or other biometrics, that we're making people less safe in a large arena of 20,000 and considering that New York City was the prime target on 9/11 that we can't prohibit individuals who have committed violence in the arena before, have been barred from the arena, now we're taking away technology that could make people around them less safe. Are you concerned at all about that?

DEPUTY COMMISSIONER BIRCHMEIER: Council Member, appreciate the question. Without talking about a specific private company, which like I said I don't feel like OTI is well-positioned to do, I think our position generally, and I think what we'd like to see kind of citywide if more of the ecosystem of governance that we have created from within government to allow for responsible use of technology and have safeguards for implementation, whether it's in the form of privacy regulations, cyber security regulations, human rights regulations, to make sure that every stakeholder is at the table if a technology is being deployed.

CHIEF PRIVACY OFFICER FITZPATRICK: To supplement that, and thank you for the question, Council Member, I think it's important from the perspective of the privacy profession, and we've talked about it, at least from the government use case, we look at lawful use, we look at mission and purpose, but we also look at principles, and it's those principles that are very important because very often as privacy professionals we find ourselves in gray areas where we have to make the best judgments that we can make, and those principles can really be guiding values, and I think what's really important, government entities learn from the private sector just as much as the private sector learns from government entities and inherent within that work I think is a direct discussion with the impacted stakeholders in the private sector which is why I think it's one of the many reasons why it's important that we're having this hearing today and having this conversation, and we're certainly interested…

COUNCIL MEMBER HOLDEN: Right. My time is up, but can I just ask one more question, Chairs?

Okay. I did want to just ask about the technology. Facial recognition has changed a lot. Has

it gotten more accurate over the years under your expertise on it, you had researched this, do you have any opinion on that?

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you for the question, Council Member. I think certainly like most technologies you see a trend towards improvement over time, but that's not to say that risk doesn't exist, right, and I think that's where the importance of governance privacy, touchpoints…

COUNCIL MEMBER HOLDEN: Right, but there's commonsense involved here because if a technology has advanced so far that we can catch the bad actors before they do something, before they commit an act of violence or terrorism or anything else, that we should employ that and we are doing it at NYPD and that's how they catch a lot of people that have committed crimes by using facial technology so we're going to deny that to businesses? I don't even know where the airport service, CLEAR, would come in here. If I signed up that I can get through an airport security quicker and I paid a fee, am I going to be prohibited, as a company doing business in New York City with CLEAR, that's another question I have. I

don't know if that bill does that, but there are certain concerns here that we're just making one fell swoop decision here and making more people less safe here so that's what my concerns are. Thank you, Chairs.

CO-CHAIRPERSON WILLIAMS: I was just asking clarity on your question. I believe that the bill has a component that would exist businesses that you have to sign up for to use that service so if I'm a CLEAR member, I signed up for it, so they would be permitted to still use the technology because I signed up to have my data used for the purposes, but, anyway, just wanted to give you clarity on that.

Next up, Council Member Hanif.

COUNCIL MEMBER HANIF: Thank you, Chair Williams, and thank you so much for testifying. I, too, will just echo the sentiments of my Colleagues for just not having adequate representation from the Administration to really thoughtfully address some of our concerns for both of the bills that are being heard today, but I will just express my gratitude for you all for acknowledging the potential of the serious discrimination that could be involved, that is involved with facial recognition and biometrics

tools, and that's really what is foundational for the bills, that we are wanting to address the discrimination, the threats to democracy that exists because of these tools. Could you expand on what types of discrimination are possible in your expert role as Chief Privacy Officer?

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you for the question, Council Member, and I certainly understand the feeling on representation though I would certainly point out that the folks that have been sent by the Administration are reflective I think of the importance with which it views this conversation. This is the first time that the Chief Privacy Officer has appeared before the Council since the role has been in existence, and I think this couldn't be a better setting for that first appearance to occur. When we look at discriminatory impact, I think what's really important and I would certainly appreciate the perspective of my Colleague from CCHR, but I think we're looking at outcomes, right, so if you're talking about the public safety space you're talking about an automated decision that's made, that's relied upon in and of itself that's resulting in liberties being taken away and

certainly I think that risk has been acknowledged I think historically with how the utilization of, for example, facial recognition has occurred within New York City in the public safety space. Any potential match is expressly identified as not equivalent to probable cause. It's merely a lead that requires further independent investigation by an investigator in a given circumstance, but I'll turn it over to my Colleague as well.

SENIOR COUNSEL SCRIVANI: Yes, thank you. I would say, yes, under the Human Rights Law it's unlawful to use this technology in a discriminatory manner. It focuses on the outcome of the use of the technological tools, but the Human Rights Law is designed to protect New Yorkers from discrimination. That applies in public accommodations, employment, and housing and to the extent that as a result of use of tool, discrimination takes place against a protected category, that could violate the New York City Human Rights Law, and protected categories, there's 27 under the Law. They include race, gender, national origin, color, religion, disability.

CHIEF PRIVACY OFFICER FITZPATRICK: I would also just supplement that. I've talked a little

bit about the reimagined citywide Privacy Protection Committee, and I just also wanted to highlight while the Commission on Human Rights is not a mandatory member of that Committee pursuant to the Identifying Information Law, they have been given a seat by Mayoral designation as a reflection of the importance of having their perspective in these conversations.

COUNCIL MEMBER HANIF: Thank you for that. I think it's very critical that our City's experts and our agencies recognize the discriminatory impacts that these tools have on everyday New Yorkers because we've heard from experts, we've read the reports and especially as someone who grew up in a post-9/11 New Yorkers with the Muslim surveillance program that tore apart Muslim communities citywide, we must recognize what the impacts are of these tools, especially when we have an Administration, we have a Mayor who while on one hand has called out the abuse of MSG in their incident and has also been in favor of using facial recognition tools in businesses and so I'd like to understand a little bit about if I could just add one or more followups. In the Admin's view, in your view, when is it appropriate for a

business to turn away a customer on the basis of a facial recognition or other biometric scan?

DEPUTY COMMISSIONER BIRCHMEIER: I would say, unfortunately, OTI doesn't have a perspective on the private business's decision. There might be private sector-facing agencies that might and the Mayor's Office might be able to give you a little bit more on that.

COUNCIL MEMBER HANIF: At this moment, there isn't any sort of standard parameters that you all have outlined somewhere…

DEPUTY COMMISSIONER BIRCHMEIER: OTI does not.

COUNCIL MEMBER HANIF: Not OTI? Just to get clarity on private businesses, they have the full authority in determining who to turn away based on these tools?

DEPUTY COMMISSIONER BIRCHMEIER: I'm not familiar enough with regulation around private businesses in general.

SENIOR COUNSEL SCRIVANI: I would just like to reiterate that if there was an intent to discriminate or also a disparate impact then that would come under the gambit of the New York City

Human Rights Law if it's based on a protected category so it's not to say I can speak to any reasons that they can but I can speak to reasons that they can't and, if they violate the Human Rights Law, then that could be businesses covered by the Human Rights Law.

COUNCIL MEMBER HANIF: Could you bring the mic a little closer to you and repeat the last bit?

SENIOR COUNSEL SCRIVANI: Yes. The Human Rights Law covers places of public accommodation which can include businesses.

COUNCIL MEMBER HANIF: Does the Admin have a position on Intro. 1014 at this time? This is banning biometrics in places of public accommodation.

DEPUTY COMMISSIONER BIRCHMEIER: OTI does not, but the Mayor's Office is happy to provide you with the Admin stance.

COUNCIL MEMBER HANIF: How soon would that…

DEPUTY COMMISSIONER BIRCHMEIER: Today.

COUNCIL MEMBER HANIF: Today?

DEPUTY COMMISSIONER BIRCHMEIER: Yeah.

COUNCIL MEMBER HANIF: Okay. I look forward to that. I'll end there.

CO-CHAIRPERSON WILLIAMS: Thank you. Council Member Paladino.

COUNCIL MEMBER PALADINO: Good afternoon and thank you very much for having this meeting. You know, normally I would be totally against any forms of what I call invasions of privacy. I hated the fact that cameras had to be put up everywhere to watch everybody's move and every action that they've taken. However, this City has come a very, very long way and not in a good way, and I'd be sitting here talking about biofacial recognition astounds me because it's something I never thought I'd ever, ever have to do, but in the police work that needs to be done today I think biofacial recognition has become a useful tool. Private businesses, that's exactly what they are. They're private. They're privately owned. Government has no business in it. So if they choose to put up these cameras or do whatever they need to do to provide the safety for their businesses because of the way they've been vandalized and theft has been rampant. Again, it's up to the individual, and it is privately owned business.

I want to know when we talk about the police work that this does do, and we discuss a lot

here about discrimination, and I don't think this is discriminatory at all as far as unique groups. I think discrimination is rampant in all nationalities so this is not something I believe any single group should ever feel singled out in because it's the reality. It's happening everywhere.

As far as the Mayor goes and the NYPD goes, they are in favor of this, and I really want to know how does this help the police do their job because they need all the help they could get.

DEPUTY COMMISSIONER BIRCHMEIER: Council Member, it's great to see you and appreciate your comments. I'd have to refer that specific comment to the NYPD to speak about their operations and how the technology can aid their operations.

COUNCIL MEMBER PALADINO: As far as landlords go, that interests me too because when a person owns a building that has, let's just say a simple building in Astoria, walk-up, three floor, four floors, whatever it is, three apartments on each floor. Again, that's private, and I think if a landlord wants to institute this, if they feel it's that necessary to do it, I think they should have the right to do it. Again, coming from me, again someone

who is against government overreach and the overextension of power, sadly I think we're in a situation where this has become a necessity and it pains me to say so. That's all I have to say I guess. Thank you.

CO-CHAIRPERSON GUTIERREZ: Thank you, Council Member.

I just had a couple of follow-up questions for OTI based on some of my Colleagues questions. I want not emphasis Local Law 63 from 2021 which in sum is mandating all property owners of multiple dwellings, which to our understanding did include NYCHA as well, that utilize these fobs or any smart technology requiring them to provide tenants with a data retention and privacy policy. Is that a Lat that you're aware of and can you say whether or not the enforcement of the distribution of said privacy policy falls within OTI?

DEPUTY COMMISSIONER BIRCHMEIER: I would say the enforcement of that specific policy does not, unless…

CHIEF PRIVACY OFFICER FITZPATRICK: That's a policy that hasn't crossed my desk during my

tenure, but I'm happy to make some inquiries in regard.

CO-CHAIRPERSON GUTIERREZ: Do you agree with it that tenants in any multiple dwelling household are at least deserving of a policy if there are cameras, if there is some kind of biometric data collection happening where they live, in lobbies, when they're entering their building for example?

CHIEF PRIVACY OFFICER FITZPATRICK: I would want to look more directly into the Law and the associated policies before providing a comment.

CO-CHAIRPERSON GUTIERREZ: So many unanswered questions today. Okay. I have one more question.

The last one is on data collected by private companies, and I think I asked this, I just need to kind of expand a little bit more on it, when private companies are collecting data, is that something that the City can purchase, can obtain, and has the City done that in these instances?

CHIEF PRIVACY OFFICER FITZPATRICK: We're certainly aware of private entities that make data available for sale. On specific instances, I'm not aware of any, but certainly what I would say is the

evaluation of those engagements they would be considered collections of identifying information pursuant to Local Law and would need to be evaluated through the lenses that we've been discussing in the course of this hearing, lawfulness, mission and purpose, and our privacy principles.

CO-CHAIRPERSON GUTIERREZ: Are there instances where city agencies are purchasing this data or are there examples of data that an agency can benefit from in wanting to obtain data from a private entity?

CHIEF PRIVACY OFFICER FITZPATRICK: I can't speak to specific instances on purchasing side but on the converse, if we're thinking about the sale of data held by city agencies, that's not something that I'm aware of as occurring and, in fact, our standard contracting language prohibits the sale of information to the extent that we are using a City vendor, for example, from that vendor reselling that information.

CO-CHAIRPERSON GUTIERREZ: Prohibits them from reselling it?

CHIEF PRIVACY OFFICER FITZPATRICK: Right.

DEPUTY COMMISSIONER BIRCHMEIER: Council Member, I would just add that I'm not aware of any city agency that is purchasing data. I'm happy to circle back with the folks at OTI and, if that is not the case, I'd be happy to correct that with you.

CO-CHAIRPERSON GUTIERREZ: Yeah. I think that would be helpful. Again, there's just a lot we don't know about not just the way data is being collected but what it's being utilized for, that's almost everyone's second question is what is it being used for, and I would just like to understand how your role is helping to kind of rectify that, especially within city agencies.

My last question is on when we had asked about NYCHA and DOE, for example, these are agencies that don't necessarily fall under your purview, but these are two examples of agencies, especially NYCHA, that have demonstrated a way of abusing biometric technology that is used. There was that attempt to bring DigiDogs into NYCHA, for example, in 2019, 2020, and tenants really like rallied around it so knowing that NYCHA tenants are very much empowered and very much informed about the way that data collection can continue to harm them and their

families. Despite you saying it doesn't really fall under OTI's purview, what recourse do tenants of NYCHA have because they are under our purview, they are tenants and residents just like everybody else and we represent them so what kind of advice can I give to a NYCHA tenant that is seeing this biometric data collection happening in their building and who do I send them to if it's not OTI? What happens there? I think your agency does have an overview or does have a reach there, but I just want to understand a little bit more because I get the Authority piece and their separate piece but then there's people piece, there's the tenant piece, and there has to be something that we at the City can do to elevate their very real and very warranted concerns around their biometric data. NYCHA is majority people of color, women and men of color, and so we're saying all these things at today's hearing, but what I'm not hearing is how to protect NYCHA tenants and I'm concerned so what are some of the things that we can tell our constituents that live in NYCHA when these fears come up? What is the City's purview to make sure that their human rights aren't being violated and that they have concern?

SENIOR COUNSEL SCRIVANI: Under the City Human Rights Law to the extent an entity is a place of public accommodation, a housing provider, or an employer, the City Human Rights Law applies when there are specific instances of discrimination so if anyone believes that they've experienced discrimination we encourage them to notify the Commission and proceed to file a complaint.

CHIEF PRIVACY OFFICER FITZPATRICK: Just to supplement that as well, we've talked about the nuanced distinction of city entities that fall within and outside of the purview of the local Identifying Information Law, but I want to emphasize to the Council that just because an entity like NYCHA or DOE, for example, falls outside the purview of the law doesn't mean that they don't have the same accessibility to my office for advice on privacy matters.

CO-CHAIRPERSON GUTIERREZ: That's what I want to know more about. That's exactly what I'm talking about. Thank you.

Council Member Williams.

CO-CHAIRPERSON WILLIAMS: Thank you. I know we've been fielding a lot of questions and some

are within our purview, some are inferred, especially with the City's Human Rights Law so just wanted to get your expert opinion around how the City should assess and address the potential for racial bias or other types of discrimination in the use of facial recognition technology.

SENIOR COUNSEL SCRIVANI: Thank you for your question, Chair Williams. I just want to say how pleased we are to be here to speak about these important issues.

The City Human Rights Law gets at the discriminatory impact or instances that can happen as a result of the use of the technology so we are certainly aware that this is a multifaceted issue, that there are issues with discrimination and privacy, and transparency and bias so when the Commission's role comes in is when there has been discrimination which can result from the use of technologies and then in those instances we encourage people to come forward to the Commission and file a complaint.

CO-CHAIRPERSON WILLIAMS: What are the potential consequences of false positive matches and how are these consequences being addressed or

mitigated? Some of the cases we were briefed on, some were in New York City, some were outside of New York City where people were falsely accused of doing a particular thing, they were arrested, and so just again wanted your opinion on potential consequences of false positive matches and if there's anything that is being done to address or mitigate those false positive matches.

SENIOR COUNSEL SCRIVANI: I can say that the use of the technology itself is somewhat outside the ambit of the Human Rights Law which is most of the time technology is being used, unless there is an instance of discrimination that results from it, it wouldn't be actionable under the Human Rights Law, but if anyone believes that they've experienced discrimination or if there is a wide-ranging disparate impact that results from use of the technologies then it would fall under the New York City Commission on Human Rights.

CO-CHAIRPERSON WILLIAMS: Okay. What happens when the technology isn't seeking to be purposefully discriminatory, maybe it's the algorithm that was created or just the lack of accuracy around a particular technology, are there any recourses

there, or is it just solely based off of the intent and usage of the particular technology?

SENIOR COUNSEL SCRIVANI: Under the New York City Human Rights Law, when there is a disparate impact on a protected category, even if a policy or practice is neutral on its face, then that can be a violation of the New York City Human Rights Law.

CHIEF PRIVACY OFFICER FITZPATRICK: If I may to supplement there, I think it's worth highlighting again, as we've been talking about, we have to acknowledge that that risk is apparent, right, and we take steps from a policy perspective to mitigate it so that's accomplished through transparency and reporting, that's accomplished by independent evaluation of algorithms that might be utilized to assess the extent to which biases operate within that particular environment, but certainly, if we're talking about from a public safety perspective, as I mentioned earlier, we've got I think standing NYPD policy, for example, relative to its use of facial recognition technology does not equate that a match equals probable cause, that there needs to be further investigation, recognizing that that risk is there and that further investigative work is

certainly needed and then, again, in the event that such circumstances would occur, for example in the public safety context, that information is disclosed appropriately so in the context of a criminal prosecution and handled as necessary in the civil context with complaints to the appropriate agency or the initiation of civil litigation.

CO-CHAIRPERSON WILLIAMS: The independent evaluation and the transparency that you mentioned, for the independent evaluation, who is conducting the independent evaluations? Are you consulting, contracting it out, or is it something that your office is doing?

CHIEF PRIVACY OFFICER FITZPATRICK: That's not something that our office is doing, but that's something that certainly will be part of the AI Action Plan that we are developing. I think the industry practice has certainly been really looking to the work that the National Institute of Standards and Technology is doing in evaluating these algorithms for bias to inform potential agency use cases in the current state.

CO-CHAIRPERSON WILLIAMS: Okay. I just want to acknowledge that we have been joined by Council Member Salamanca.

Just to make sure I heard you correctly, there's a plan to potentially carry out the things that you just mentioned to mitigate any potential discriminatory practices with the technology through the AI Action Plan?

CHIEF PRIVACY OFFICER FITZPATRICK: That would be a component part of the AI Action Plan.

CO-CHAIRPERSON WILLIAMS: Okay. Thank you. The other question I have is what types of data collection or use limitation should be in place, if any, to ensure that facial recognition technology is not used to infringe on First Amendment rights such as freedom of speech or assembly. There were tons of reports that during the BLM protests there was various forms of surveillance that was used, and so if you could share what those limitations might be in reference to infringing upon the First Amendment rights?

CHIEF PRIVACY OFFICER FITZPATRICK: Sure, absolutely. I think if we're talking about the public safety context, NYPD is certainly best positioned to

speak to that, but obviously the First Amendment context is an extraordinarily sensitive one, and New York City NYPD operations in the space of political activity have been governed by a longstanding federal consent decree known as the Handschu Consent Decree, which provides for a framework for how investigations involving political activity may occur by the Department, and the current state of that consent decree also includes the integration of an independent civilian representative who has a seat at the table to facilitate compliance with the Consent Decree and any engagements that may be necessary to flag violations of it to the overseeing federal court judge.

CO-CHAIRPERSON WILLIAMS: What you're talking about, is that the Handschu Committee or is this something different?

CHIEF PRIVACY OFFICER FITZPATRICK: That's correct. That's the Handschu.

CO-CHAIRPERSON WILLIAMS: Okay, so one of the things with that which was here in the briefing documents is that the Handschu Committee was not a part of the recent surveillance practices of the Black Lives Matters protests so I know this is not

really your purview, but it seems as though that Committee is not being used in all aspects of surveillance and it's only used in particular aspects of surveillance.

CHIEF PRIVACY OFFICER FITZPATRICK: For the specific use cases, there again I'd have to refer you to the NYPD for specifics.

CO-CHAIRPERSON WILLIAMS: No problem. The next questions I have are around limitations and restrictions on facial recognition technology in sensitive locations such as schools, places of worship, abortion clinics, or public protests. We've been talking about public protests. If you could just give us your broad opinion, and this could be CCHR or OTI on what you recommend the Council consider such limitations to protect privacy and safety of individuals so this could be an agency by way of the NYPD and/or private actors that might want to use this technology and have there been any reported instances of using facial recognition technology at such sensitive locations to CCHR or any other city entity?

SENIOR COUNSEL SCRIVANI: As far as the privacy aspect, that's somewhat outside the purview

of the City Human Rights Law, and I know there's a lot of issues that are coming up, equity, discrimination, transparency, privacy, but I want to be clear that unless it's involving discrimination it really isn't in the purview of the Commission. Again, just reiterating that the Commission's role comes in when, generally most uses of technology wouldn't be a violation of the City Human Rights Law, but if they're used in a discriminatory manner, that's when it would come to the Commission.

CO-CHAIRPERSON WILLIAMS: Have you seen any cases?

SENIOR COUNSEL SCRIVANI: We have not had any cases where allegations of discrimination based on facial recognition have come to us. The closest thing, we have had a case where artificial intelligence was a factor in alleged discrimination, and that involved a website using an algorithm that had a discriminatory impact on a protected category.

CO-CHAIRPERSON WILLIAMS: What happened in that case?

SENIOR COUNSEL SCRIVANI: The case was resolved via settlement, and, as part of the settlement, the website had to incorporate some human

interaction so it wasn't just the algorithms at play which resulted in the discrimination.

CO-CHAIRPERSON WILLIAMS: Thank you. Do any of my Colleagues have any… Council Member Hanif.

COUNCIL MEMBER HANIF: Thank you. Could you share how many businesses are currently disclosing their use of biometric technology pursuant to Local Law 3 of 2021?

CHIEF PRIVACY OFFICER FITZPATRICK: That's not information that my office maintains or has visibility into.

COUNCIL MEMBER HANIF: Who would have this information?

DEPUTY COMMISSIONER BIRCHMEIER: I'm not sure if it's collected.

COUNCIL MEMBER HANIF: Got it. I'm just trying to understand sort of how the City does interact with this Law.

Second, how is the Administration holding companies who use biometric technology without disclosing as required by Law accountable?

CHIEF PRIVACY OFFICER FITZPATRICK: I'm not aware of specific enforcement actions by the Administration, though certainly my understanding is

that the Law at issue affords impacted entities from bringing private rights of action independently against offending parties.

COUNCIL MEMBER HANIF: Against?

CHIEF PRIVACY OFFICER FITZPATRICK: Offending parties.

COUNCIL MEMBER HANIF: Offending parties. Was that the one complaint that came up earlier in the conversation today?

CHIEF PRIVACY OFFICER FITZPATRICK: No.

COUNCIL MEMBER HANIF: Okay. Could you describe a little bit, more clarify what that was referring to?

CHIEF PRIVACY OFFICER FITZPATRICK: Sure. The specific instance at issue, I received engagement from a member of the public that a particular city agency had disclosed identifying information in the course of a legal proceeding and raising concerns about the nature of that disclosure. In response, I and my office engaged the privacy officer at the particular agency to get an understanding of the specific circumstances in which that occurred and certainly to enable an agency-level investigation into it.

COUNCIL MEMBER HANIF: Okay. How does the public know to report violations of privacy?

CHIEF PRIVACY OFFICER FITZPATRICK: The Identifying Information Law affords for a mechanism for the public to engage with us, and that's enabled through the OTI webpage.

COUNCIL MEMBER HANIF: OTI webpage, but there isn't a sort of campaign like if you feel that your privacy is under attack or…

CHIEF PRIVACY OFFICER FITZPATRICK: I wouldn't say specifically through that lens, though one of the areas that, and I'm very appreciative of the support of this Administration, is the efforts that it's made in putting the work of the Privacy Office and the existence of the Privacy Office into more public-facing settings such as this one to make sure that folks are aware that New York City actually does have a CPO and what those responsibilities are.

COUNCIL MEMBER HANIF: Great. What about for CCHR? On this question but to CCHR, if a New Yorker wants to report, is there material for New Yorkers to know that they can do this, that they should not feel any threat around repercussions when

they feel that there's been a violation of their privacy?

SENIOR COUNSEL SCRIVANI: The issue of violation of privacy rights is outside of the Human Rights Law which is really addressing discrimination against protected categories in employment, places of public accommodation, and housing, but as far as materials as part of our Agency's mission and mandate, we are constantly educating the public, both the covered entities who are subject to obligations and New Yorkers who gain protection from the City Human Rights Law about their rights and also about their right to be free from retaliation and how to file complaints.

COUNCIL MEMBER HANIF: Thank you. That's it.

CO-CHAIRPERSON GUTIERREZ: Thank you, Council Members. No other Member has questions?

I will just conclude by saying I appreciate you all being here, nice to meet you. So many of our questions are unanswered, and I'm disappointed because we tried to frame them centering concerns from our constituencies and our Districts, and I've said this before but I hope that when you

come again that you'll be able to share some of those answers, even in the meantime to send them over. I think we've got a record amount of advocates signed up to speak. You likely won't stay to hear their questions, but I think it's really important that when we come to these hearings that we're entering to the best of our ability. You're OTI. People want to hear the data. We want to hear all of that, and that's really important, and I don't ever want to waste anybody's time here so thank you for the answers that you were able to provide and looking forward to hearing back from some of the ones that you were not able to do so today.

CHIEF PRIVACY OFFICER FITZPATRICK: Absolutely, and you can count on that, and thank you, Council Member, for having us and thank you to all Members of the Council for the conversation today.

CO-CHAIRPERSON GUTIERREZ: Thank you very much.

COMMITTEE COUNSEL BYHOVSKY: Thank you, everyone, for your testimonies and insight, and now we move to the testimony from the public.

We'll start with witnesses who are here today in person and then call witnesses who are here virtually.

Before we begin, I also would like to acknowledge that we have received written testimonies from the public including the Real Estate Board of New York, Food Industry Alliance of New York State, Tech NYC on behalf of its clients, Mobilization for Justice, Partnership for New York City, and (INAUDIBLE) and others.

If any member of the public wishes to submit written testimony, you can do that by emailing to testimony@council.nyc.gov.

Now, I want to welcome our first panel, and our first panel is Daniel Schwartz, Albert Fox Cahn, and Alli Finn.

To accommodate all witnesses, we kindly ask to limit your testimony to three minutes. Thank you.

DANIEL SCHWARTZ: Thank you. My name is Daniel Schwartz, and I'm testifying on behalf of the New York Civil Liberties Union. We thank the Committee and Council Members 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 are also highly flawed and racially biased. The widespread use of these technologies presents a clear danger to all New Yorkers' civil liberties and threatens to erode our fundamental rights to privacy, protests, and equal treatment under the law.

The Council must ensure New Yorkers are not surveilled, targeted, discriminated against, and criminalized on the basis of invasive, flawed, and biased technology. To this end, we call for prohibitions on biometric surveillance in areas of severe power imbalance including its use by law enforcement or other government agencies, in housing, and in other areas where our fundamental rights are at stake or where informed consent cannot be given.

Intro. 1014 would prohibit places of public accommodations from using biometric recognition, and it would require written consent for any collection of biometric data. It would create transparency, security, and deletion requirements and

ensure that customers are not treated or charged differently because they do not consent to the collection of their biometric data. The facial recognition deployment by MSG Entertainment to target staff from law firms in litigation with MSG points to Orwellian use cases where it will be impossible to move and associate freely, and the technology's racial as well as gender bias risks disproportionately impacting women and people of color such as a misidentification of a black teenager that barred her from entering an ice-skating rink. For these reasons, we support banning biometric surveillance in places of public accommodations. Furthermore, visiting retail stores, restaurants, museums, entertainment venues, or healthcare sites should not automatically open one up for the collection of sensitive biometric information without prior informed consent and clear rules for access, use, security, retention, and deletion.

To ensure that the legislation fully meets its goals, we make detailed recommendations in our written testimony. In brief, we recommend the coverage to apply to all individuals, not just customers. The policies should be required to be

publicly available outright rather than conditioning the availability on a request. Finally, the private right of action must be further strengthened as an accountability and enforcement tool.

On Intro. 1024, it would prevent landlords from using biometric recognition technology. The deployment of biometric surveillance risks conditioning entry into one's home, the place where our Constitutional rights are at the most robust, on the provision of one's most sensitive biological data. Residents should not have to live in fear that landlords are tracking their comings and goings and amassing sensitive data on them and their guests. Not only does biometric surveillance in residential buildings cause harm to tenants' privacy rights but also their civil rights to access housing on equal and nondiscriminatory terms. Notably missing from this bill, I'm almost done, is a private right of action that would provide tenants and their guests with a tool to hold landlords accountable. Without it, there would be no recourse for affected people and likely no enforcement against violating landlords. Given the City's housing crisis, we strongly recommend the addition of a private right of

action and as a crucial enforcement and accountability mechanism.

Nobody wants to live in a world where pervasive surveillance identifies them, tracks their movements and associations, and impacts which places they can visit, which services they can access, with whom they meet, or how to exercise their free speech rights. The NYCLU supports Intro. 1014 and 1024, and we urge their swift passage. Thank you.

ALBERT FOX CAHN: Good afternoon. My name is Albert Fox Cahn, and I'm the Executive Director of STOP, the Surveillance Technology Oversight Project. We are a New York-based privacy and civil rights group. I have a statement for the record that I've submitted that details why we believe that Intros 1014 and 1024 are indispensable safeguards for New Yorkers, but I also need to respond to some of the misinformation we have heard from the Administration officials in this very hearing. We have heard that New York City doesn't provide information about New Yorkers to private companies. This despite the fact that historically the NYPD provided facial recognition training data to IBM so it could better develop facial recognition software to track black

and Latinx individuals. We heard that they didn't know if we had the City obtaining information from private companies even though the NYPD has access to more than 30,000 cameras through the Domain Awareness System. We heard how equity was a value that was driving the City's policy, but when my organization asked the NYPD for its data on the bias and accuracy of its own facial recognition system under Freedom of Information as described in this hearing we were told not only that they wouldn't provide any records but that the records didn't exist, that they truly had no information about whether or not their own facial recognition system was biased. This was submitted under oath by NYPD officials, and we are continuing to litigate that matter. We heard about how there are all these commitments to transparency despite the fact that the Office of the Inspector General recently came out with a report saying that the NYPD has failed to correct 93 percent of the deficiencies found in the NYPD's implementation of the POST Act. The NYPD is systematically breaking transparency and oversight laws and, while it's great that we have identifying information protections under City law as was described with Public Law 247, there is no

mention of the fact that there is a carveout that you can drive a truck through, that it exempts information disclosed for law enforcement purposes, so again we are told this narrative that New Yorkers' privacy is being protected when in practice it is a free-for-all. There are no meaningful safeguards, and that's why these sorts of protections, why we need these sorts of laws to defend against the consistent growth of facial recognition.

I want to highlight that given this track record, we cannot trust the Administration to enforce these laws. Arguably, Human Rights Law already outlaws facial recognition because it is discriminatory and barring access to a place of public accommodation, but that has never been enforced, and that's why we need a private right of action in both these bills. Thank you.

ALLI FINN: Hi. My name is Alli Finn. I'm testifying today on behalf of the Surveillance Resistance Lab, an NYC-based organization that focuses on corporate and state surveillance systems as one of the greatest threats to democracy, migrant rights, economic justice, racial equity, and economic justice. I'm also going to go off script because I'm

so concerned by a lot of what OTI shared today. OTI said that they are not aware of city agencies purchasing our private data from private entities. We have a lot of questions about how this works, but we know it is happening. For example, Data Miner, which is a social media surveillance company and data broker which there have been numerous news reports about how Data Miner extracts social media data to surveil and help police target Black Lives Matter protesters in the wake of George Floyd's murder. Data Miner contracts with NYPD as well as the Office of Emergency Management. LexisNexis, one of the most notorious data brokers, which helps ICE profile, track, identify immigrants for detention and deportation, also contracts not only with the NYPD but numerous city agencies, and we have a lot of unanswered questions about how much of our city data is going into LexisNexis' profiling systems as well as partnerships that are not necessarily written down in contracts but arrangements such as sharing data from Ring cameras, the NYPD, all 77 precincts, have an MOU with Ring that is not a paid agreement for access to some of that footage.

Putting that aside, I just want to say that biometric surveillance tech including facial recognition is a monumental threat to democracy and peoples' rights and security, not only privacy, so we urgently call on the City Council to pass these two essential bills as well as a full ban on government use. There is no other option. Facial recognition is so dangerous that its use cannot be justified even when it helps some people in this room feel safe. Biometric surveillance has been increasingly weaponized in our city and worldwide to take away peoples' rights, liberties, and access to basic resources. This includes criminalizing poverty, facilitating mass arrests and incarceration of BIPOC communities, surveilling protesters, and targeting immigrants for deportation, and increased accuracy rates will never, ever fix these harms because tech and algorithms are not neutral and they reflect the biases of the people behind them and the systems that use them. I'm going through this real fast.

Lastly, I just want to say that biometric surveillance does not only rely on the collection of faceprints and our other data, our iris scans, etc., but unregulated mass data-sharing systems that

drastically exacerbate these risks, and that's why I wanted to highlight what OTI failed to mention today. We would love to work with the City Council to investigate these harms, to investigate mass data-sharing and how these surveillance systems interact with those webs as well which actively materially harm New Yorkers. Thank you.

CO-CHAIRPERSON GUTIERREZ: Thank you. Yes, I would love to have that conversation and build out. Obviously, I was very disappointed, I think a few of the Members also shared how disappointed with the level of preparation that OTI came here with today, although I'm not surprised. Their interest is in protecting what they do, but our responsibility here is to continue to demand and push that they be more transparent and accountable. I have two questions for you all as you are advocates but the experts. Are there any positive examples of the use of facial recognition technology besides like our iPhones being able to open it, but do they exist, and then my second question is, obviously I'm in support of both bills, but can you share what are some of the risks of storage of biometric information by private entities like landlords for example?

ALBERT FOX CAHN: Just to quickly touch on those points. If your credit card number is hacked, you can change your credit card. If your Social Security Number is compromised, you can even change that. You can't change your biometric data. If it is compromised, it is compromised for life, and it will be a persistent threat to your privacy, to your cyber security. As far as good uses of facial recognition, I think that there is a world of difference between voluntarily using facial recognition on your own phone as a matter of convenience versus having it used against you as a surveillance tool by those who have power over you, and the power differential is key here. That's why we're talking about places of public accommodation, that's why we're talking about landlords, because these are core environments where you potentially see technology augmenting systemic discrimination and just a lengthy inability that tenants and customers have had to exercise their rights.

DANIEL SCHWARTZ: In addition to what Albert just mentioned, I think the BIPA, Biometric Information Privacy Act, in Illinois is a great example of how biometric privacy protections can work

and why it's so crucial to have informed consent with transparency on the privacy policies as Intro. 1014 would required, clear guidelines on retention, deletion schedules, and really making clear that in those use cases that are covered by Intro. 1014 and 1024 informed consent cannot be given because as Local Law 3 has exemplified since it came into effect it's not meaningful, people are oftentimes not informed, and there's no other way than outlawing it and prohibiting it in those circumstances and ensuring that the collection of biometric and storage of biometric data only happens on a narrowly defined and with a provision of clear rights to affected people.

ALLI FINN: Thank you so much, Chair, for your questions. I agree about Illinois' law. It's one of the strongest ones we have in the country, and there's numerous jurisdictions that are legislating responsibly about this, and many of those are full bans. I do want to say no opt-out regimen is ever going to keep people safe. Opt-in, there's a lot of debate about that. I don't have a lot of positive use cases for you, but gold standard would include opt-

in, never any opt-out to put the burden on the resident.

You also asked about risks of storage by private entities. These are numerous, largely because it's not only at the local level that we don't have adequate protections. We don't have adequate protections or any protections really at the State or the Federal level so when we're talking about private entities that extract, store, share, and sell our biometrics and other personal data there's virtually no restrictions about how they would treat that data, who they share it with, where it goes, the extent of where it is sold, and we don't know the full extent of it. In addition, ransomware attacks and cyber security attacks are increasing on municipalities. Some of what Baltimore dealt with is a really terrifying example of that and, just like Albert said, this is not information that can easily be changed. You're stuck with your iris scan and your faceprint pretty much forever, and we cannot take these risks because the NYPD wants to feed the Domain Awareness system and because landlords want to drive out rent-subsidized and low-income tenants.

ALBERT FOX CAHN: If I could just add, on a personal note, I recently rented an apartment, and I tried very hard to find one that wouldn't collect my biometric data. I couldn't and so every day I have to go into a building where my data is being taken without my consent and without even the bare notice that's required under existing laws so notice is not enough because it's simply not being honored.

CO-CHAIRPERSON GUTIERREZ: Thank you. Council Member Hanif had questions?

COUNCIL MEMBER HANIF: Yes. Thank you so much for just teaching us so much about biometrics and facial recognition tools and just how they directly breech our privacy and threaten democracy. Could you share if, right now like the expectation for me, for us is that some store has collected my biometrics. Can I just assume that I've gone to a grocery store, I've gone to a shop that already has my details, my data? What does this mean for me? What does this mean for a New Yorker day to day?

DANIEL SCHWARTZ: Unfortunately, as the Administration already earlier mentioned, they don't keep track of who's deploying biometric surveillance systems, and we don't have a database of that either.

We know of some instances of large corporations, obviously the famous reporting and deployment of MSG has been a case in point, other corporations have posted since also at Kashmir Hill at the New York Times had some great reporting in the followup to the Council hearing in February regarding biometric disclosure law in New York City, but what it means, I think it really depends. We see the rise of centralized data collections by some of those surveillance vendors that would be able to really analyze customer and people's behavior of which stores they visit, how they spend their time, what they're interested in, and target them very specifically. We see with MSG where it scraped all the law firm's staff pages and LinkedIn pages for profile photos of people that work at law firms that are in litigation with them and denied them entrance to the venues that are under their control, and I think that is just the tip of the iceberg. In my testimony, the case of a black teenager that was denied entrance because of a misidentification of her that flagged her as having been involved in a fight but she had never been before to that ice-skating rink, and she was denied entrance and had to wait for

her parents to pick her up afterwards, and I think in the vast majority of cases people will never know that their information is being collected, there are profiles created about them, and I think that's also why we only know about so few cases nationally, and the cases that we do know about, the six publicly known cases of false arrests or where people were arrested because of facial recognition misidentifications, all six of them were black men, and where we know the software is utilized, it was DataWorks Plus, what was mentioned earlier in the testimony by OTI that is used by the NYPD, and Clearview AI which also has been used by the NYPD.

ALLI FINN: Thank you for the question. I think similar to other forms of surveillance, biometrics collection and facial recognition is about power, and who holds those technologies are those whose power is being increased. You, yourself, mentioned the history of post-9/11 surveillance in the city on Muslim, Arabs, South Asian, and other communities. The Department of Homeland Security's establishment after 9/11 drastically increased funding and rhetoric and support for surveillance across the country including in New York City, and a

lot of that surveillance is based on targeting people who those in power at the time decide is a threat, and that threat can change, and what that means is that surveillance doesn't target everyone equally. These are a threat to all of our rights, but, of course, it is targeting certain groups of people more, and the City Council has a responsibility to protect people of color, to protect Muslim, Arab, South Asian communities, to protect trans and queer communities, low-income communities, the list goes on. What it means for you as a New Yorker depends a little bit on who you are and where you live, and I think that's important to not skate over. MSG showed how a company can decide that a lawyer is a threat because of where they work and deny them the opportunity to see a performance with their child, but it also shows that surveillance can be easily weaponized in so many other iterations. Business owners can racially profile shoppers and call the police on someone simply for what they look like for walking into a store and landlords can criminalize and limit who comes and goes and, like Council Members have mentioned, deny people housing and increase eviction rates and gentrification so I can

monologue about this for a while, but I'll pass it on.

ALBERT FOX CAHN: I think the sad truth is no one can tell you the complete answer because the technology is going to continue to evolve, it's going to continue to proliferate, and your biometrics won't change, and so a biometric violation today can impact your safety, your security, your autonomy 10 years, 20 years, 30 years from now, and I have no idea what the technology will be capable of then, I have no idea how it will be used, and so it's really that timeframe of harm here that I think sets biometric surveillance apart. There's a lot of data that's collected about us constantly, but this is the one piece of data that will stick with us for the rest of our lives.

COUNCIL MEMBER HANIF: Are there positive uses for biometrics and facial recognition tools, and, if so, what are they?

ALBERT FOX CAHN: Again, I think there's a difference between when you consent to use biometrics on your own device as a point of convenience versus when there's a power dynamic between the person installing the biometric surveillance and the person

being watched. Landlords aren't tracking themselves with the same technology. Oftentimes, they are installing it track tenants and not the other way around. Business owners are not being tracked with this technology; the customers are. So I think really you can never at a technology divorced from the power dynamics of how it's used.

ALLI FINN: We get this question a lot including from folks at the NYPD when we raise concerns, and I just want to say just because a technology exists doesn't mean we have to use it. It doesn't mean that it's the solution. Just because a company is selling a product doesn't mean that we have to buy it and apply it to New Yorkers' lives so when I get asked that question I like to talk about other things that I would like to see our City invest its resources in like housing, like schools, like a lot of what the Mayor has cut budget from rather than technologies that serve corporate and carceral interests.

DANIEL SCHWARTZ: I would just add that the few use cases that are often marketed with and are used to justify the deployment of biometric surveillance don't weigh against all the harms that

we're seeing, and, as I mentioned earlier, we only know of the tip of the iceberg because most of the people are never made aware whether facial recognition was used for example in their arrest, in their identification, and facial recognition and biometric surveillance at large, it's dangerous when it works as we see in the MSG deployment, and it is harmful when it doesn't work because of all the racial and gender bias that we have mentioned.

COUNCIL MEMBER HANIF: Finally, the companies that are like scraping this data and like investing in biometrics and facial recognition tools, is this a growing base of companies, are we seeing more of these companies, and do you have the research like who are the most egregious companies or most popular companies in New York City given the Admin really had no answer to that but since you all do this research day-in and day-out would love for the Council to receive some of the names of these companies to learn a little bit more?

DAVID SCHWARTZ: It's a vast field, and it's only growing because of the lack of regulations. I mentioned BIPA earlier. Under BIPA, fortunately, there was a settlement against Clearview AI, one of

the most infamous surveillance vendors that has amassed more than, by their own account, 20 billion social media images so basically anyone that has ever used a social media platform, whether it's Facebook, Twitter, Instagram, LinkedIn, and hadn't locked down the privacy settings and had some photos publicly available, that person is likely to be included in the database and could be in the crosshairs of paying customers of Clearview AI. Many of the large tech companies have their own biometric surveillance systems. There's a number of algorithms that are out there, and even small startups have scaled up, and I think it's impossible to track at this point all the names of vendors because there's literally hundreds. NIST was mentioned earlier by OTI about how they're evaluating and doing audits on the accuracy, and that test has grown in size, but they have also found the bias, specifically the racial bias, that we note in literally all the vendors across the board.

ALLI FINN: I just want to highlight this even further, that we don't know the full list of vendors that the City is contracting with. Going back to Fiscal Year 2010, there are almost 5 million anonymized spending records in the City's procurement

database. That means that the vendor is not named. This is across all agencies. We do not know the scope of these contracts.

To answer the other part of your question, this is an extremely lucrative industry that is only growing because of this lack of regulation and because of the money there is to be made because of the increasing list of customers for these vendors, and a lot of times when cities and agencies are contracting with vendors focused on surveillance- and data-driven technologies, they are not only using data that comes from those vendors but they're providing that information so law enforcement data is shared, private information is shared. I'm happy to go into more detail.

ALBERT FOX CAHN: While there is a relatively small number of companies that offer physical entry devices for buildings that integrate facial recognition. It's a growing universe, but it's comparatively small, but there's a huge number of apps and websites and software providers, many of which are based outside the U.S. and operate without any compliance with our minimal privacy laws here in the U.S. and will offer facial recognition services.

A key thing to remember is that every camera is just one software upgrade away from being used for facial recognition. You can take a photo from just a traditional CCTV camera, from an employee's cell phone, from anywhere and run it through websites that for 20 bucks I can go and take that photo and figure out someone's identity. It's that unregulated today, and really I think when you look at the full range of businesses in New York there probably are thousands of different facial recognition products and other biometric products being used.

CO-CHAIRPERSON WILLIAMS: Thank you. I just want to make sure I heard you correctly. Did you say that city agencies are contracting with these companies?

ALLI FINN: Could you clarify the question?

CO-CHAIRPERSON WILLIAMS: Yeah. You said something about companies and something about the agencies are contracting with…

ALLI FINN: Yeah. I'm not sure if this is what you're referring to. We've been looking at City procurement data since Fiscal Year 2010 simply because that's when the bulk of it has been made

available online, and what we're finding is there's close to 5 million spending records where the vendor has been anonymized across city agencies so maybe the Comptroller has access to that, maybe other city agencies have access to that, but we, as the public, do not know who those vendors are. Some of those could be surveillance and policing technologies. Was that the question you were referring to?

CO-CHAIRPERSON WILLIAMS: Yeah. You said 5 million vendors or…

ALLI FINN: Close to 5 million records, spending records, so some of those can be under the same contracts, but we have been asking questions about this, and we'd love to ask more.

CO-CHAIRPERSON WILLIAMS: Where did you say that was (INAUDIBLE)

ALLI FINN: It's in the Checkbook, the online public database of NYC procurement. They're under NA Privacy Security. That is the name of the vendor in all of those cases.

CO-CHAIRPERSON WILLIAMS: You said it was NY Security?

ALLI FINN: NA like not applicable privacy security. This is also not in the procurement rules so we would love to investigate this further.

ALBERT FOX CAHN: I should mention last year the Legal Aid Society and my organization released about 3 billion dollars in formerly secret NYPD contracts that had been hidden from the public under what was called the Special Expenses Program. This was a program in collaboration with the Comptroller's Office that allowed them to redact contracts that were being entered into on privacy grounds and so we see a number of these programs to shield contractors, and we also see that the NYPD Foundation is being used as a workaround to avoid having contracts publicly recorded, and there's extensive use of trial accounts so Clearview AI, the NYPD was explicit in the past that they never had a contract with Clearview AI but later was leaked that they were the top user of the platform at the time because they had so many trial accounts that they had officers running thousands of searches and when officers got access to Clearview AI trial, they got an email saying essentially don't just run one or two

searches, try running a dozen and see how good it is. It was really an invitation to abuse the software.

CO-CHAIRPERSON WILLIAMS: Thank you. I was just wondering because I know that the Administration testified when asked a question about the usage of consultants that are providing this, and they kind of made it seem like they don't know or the City was potentially using those resources. Okay.

Are you done with your questions, Council Member Hanif? I believe you were. If so, Richardson Jordan was next.

COUNCIL MEMBER RICHARDSON JORDAN: Thank you for coming. Thank you for waiting. Thank you for your testimony. I appreciated the information because I honestly picked up a lot, and I just wanted to ask you because you're advocates and you're informed in this space, how would you combat the narrative around policing and crime? How would you argue about the values that we're speaking about to end the surveillance in the context of people saying that we need to do the biometrics to stop crime?

ALBERT FOX CAHN: I think it's important for people to understand just how error-prone facial recognition is. In addition to the algorithm being

biased in many cases, you also see a lot of pseudoscience so the standard procedure for the NYPD has historically been that they'll get an image and if the eyes are closed they'll photoshop them open, if the mouth is open they'll photoshop it closed, and in some cases they've even gone onto Google and typed in the phrase black male model, found the face of a random individual, copied the jawline of that individual onto the image from the crime scene, and then put that collage through the facial recognition algorithm, and that led to an arrest, and so you see a lot of these practices. I'm sure you'll hear from technology industry professionals later about how algorithm might be improving or might be changing, but the algorithm is just one source of what's driving the error here, and so it's not a question about choosing between our Constitution and our safety, it's a question of whether we're going to allow the City and for these businesses to continue to waste huge amounts of money on technology that is putting New Yorkers in harm's way. I just think that as we've seen all too often with the Administration's rhetoric on surveillance, whether it's ShotSpotter or handing out Air Tags as a way to prevent car theft

even though they've been routinely abused to stalk members of the public, that they're looking for the rhetoric of a quick tech fix but all too often the tech isn't up to the job.

ALLI FINN: I think that as more and more people look for alternative approaches to policing that can be inherently violent, there is a push towards technology and towards surveillance and that can be tempting, but what I always talk about with people is it's really important to remember that surveillance is a form of policing. It has always been in service of policing. Oftentimes what people experience on their bodies is a direct result of tech-supported surveillance that led to that moment whether it is an ICE arrest or someone being racially profiled and physically harmed by the police, it plays a role, so I think there's a difference between surveillance cameras making some people feel safe and what safety actually is. Do they prevent theft from happening or harm from happening? No, but they have the illusion and push us further away from the interventions that our communities desperately need that are actual public safety.

DANIEL SCHWARTZ: Maybe just to add on both Alli's and Albert's points, a lot of the use cases are also not for what it's (INAUDIBLE) like they will prevent terrorist attacks or other really serious forms of crime and incidents here in New York, but we see this technology used against like minor theft of like, for example, a man was identified through facial recognition and he was stealing bottles of beer at a corner store. How did they actually use the facial recognition in that incident? They used again these completely unscientific methods and used a celebrity lookalike because they thought this person looked like Woody Harrelson and so the CCTV footage was so grainy and then at an angle, bad resolution, so instead of using the original CCTV capture, they googled the actor and utilized the high-resolution portrait of the actor instead.

COUNCIL MEMBER RICHARDSON JORDAN: Thank you.

CO-CHAIRPERSON WILLIAMS: Council Member Holden.

COUNCIL MEMBER HOLDEN: Thank you. Just to clarify, you're against, and this is yes or no, you

don't have to go into a long explanation, but are you against the ARGUS, the police ARGUS cameras that we paid 35,000 as Council Members to post in the neighborhoods?

ALBERT FOX CAHN: Yes, I'm against the use…

COUNCIL MEMBER HOLDEN: You're against.

ALBERT FOX CAHN: Of those cameras because they haven't been shown to actually…

COUNCIL MEMBER HOLDEN: No, I would imagine. Go ahead.

DANIEL SCHWARTZ: Which cameras?

COUNCIL MEMBER HOLDEN: ARGUS, the police cameras that we see.

DANIEL SCHWARTZ: I think it depends on the specific details…

COUNCIL MEMBER HOLDEN: These are surveillance cameras that on the streets of New York City, all over. There are thousands of them.

DANIEL SCHWARTZ: Yeah, against.

COUNCIL MEMBER HOLDEN: You're against it?

ALLI FINN: Yes, we don't need them.

COUNCIL MEMBER HOLDEN: You don't need them either? Are you against the red light cameras?

DANIEL SCHWARTZ: As long as the privacy protections are there, so it really depends on the limitations both from…

COUNCIL MEMBER HOLDEN: Red light cameras, speeding cameras, you'd be okay with?

DANIEL SCHWARTZ: It depends. There's both protections from the technological side and the policy side. For example, if those are met…

COUNCIL MEMBER HOLDEN: I just want a yes or a no.

DANIEL SCHWARTZ: There's no simple yes or no because there's such a wide range of…

COUNCIL MEMBER HOLDEN: You know what a red light camera does?

DANIEL SCHWARTZ: Yes, but there's different products, and so as long as the protection…

COUNCIL MEMBER HOLDEN: It gets your license plate and it sends you a fine. What about you? Are you against?

ALLI FINN: I agree with Daniel that these are complex issues.

COUNCIL MEMBER HOLDEN: They're complex issues when we talk about running a red light but not

for catching a mass murderer with the ARGUS cameras, right?

ALLI FINN: I think it goes down to, again, who has access to that data and what is being done with.

COUNCIL MEMBER HOLDEN: Okay, so let's say the person who just killed three kids, we use facial recognition to get him, to arrest that person, that's not good? Is that what you're saying?

ALBERT FOX CAHN: Council Member, that's a horrific hypothetical, but the truth is this is being used to arrest people for shoplifting beer, like we can always talk about the…

COUNCIL MEMBER HOLDEN: I know, but there is a thing called where we have the technology and we could actually put somebody away that could protect us on the streets of New York City from this person repeating the crime and the fact that all three of you seem to be against an ARGUS camera is ludicrous, that's my opinion, but the second thing. You also mentioned about the Ring cameras. Do you know the NYPD had an agreement with Ring, people posted their Ring information online, they put it online for other people to see to warn people against people that were

stealing packages or coming in their yard and trespassing so I posted, let's say, because I'm on the Ring network to warn my neighbors, and you're using that as an example of how the NYPD is infringing on people. This is ludicrous. This gets to a point where you're not mentioning everything, you're just picking and choosing, like you're for the speed cameras, sort of, some are not, but you're against cameras that can put murderers away or at least catch them, get them off the streets. Okay, thank you, Chair. I mean it's just mindboggling.

ALBERT FOX CAHN: Can I briefly respond, Chair?

CO-CHAIRPERSON WILLIAMS: Sure. Briefly.

ALBERT FOX CAHN: I just want to point out in recent weeks there was an individual who refused to give police Ring camera footage about their neighbor and received a warrant for all the Ring camera footage, not just of their neighbor's house but from within their own house. There is so much potential for abuse with any of these systems, even something as simple as a Ring camera.

COUNCIL MEMBER HOLDEN: That's slightly different. That's a different situation. I'm talking

about what you had mentioned, I think you had mentioned or it's in your testimony, that the Ring issue was some kind of nefarious conspiracy by the NYPD. These are things that are posted on social media that everyone can see. That's what I'm mentioning. I didn't mention anything about other agreements that the NYPD did, but, see, we have to get the whole picture here, and by withholding certain things it's not really a wise thing. We do have cameras for a reason. I've never had a constituent, by the way, ask me to take a camera out. They want more cameras on the streets, and your extreme views on this is troubling because you can't pick and choose I like the speed camera or the red light camera, some of you have done that, or I don't like where we can catch a murderer. Come on. Are we living in a bizarro world here sometimes? I understand technology has to be controlled. I understand that, but we get to a point where if it really makes us safe and not feel safer, when it really makes us safe, that I don't want somebody placing a bomb in Madison Square Garden. If facial recognition stops that, then I'd be for it. I have nothing to hide. You put a sign up, there's facial

recognition, you don't want to come in, don't come in. You don't want to go into the store, don't go into the store. Going the other way, you're going to infringe on the rights of the rest of us. Thank you, Chair.

CO-CHAIRPERSON WILLIAMS: Thank you, Council Member Holden.

Okay, I have some questions as well, but I just wanted to let my Colleagues to go. If you could share with us the harms of potentially linking data? I think it's one thing to have facial recognition data but then it's another thing when data gets linked so are you able to share with us the harms of linking data, especially biometric data?

ALBERT FOX CAHN: Yeah. When you combine and link data, you're multiplying the impact it has if that data is breached, if it's disclosed, if it's accessed by a third party. When you see vendors like LexisNexis or Thompson Reuters compiling dossiers, each of these data points may seem innocuous on its own but the danger posed by the amalgamation of all this data is greater than the sum of its parts. I would say that you're creating an even greater impact when you link data.

ALLI FINN: Just to add to that, the other danger is that in many cases what we see is it's not only people's datapoints that are getting linked, their biometrics, their biographics, right, their home address, where they live, what they do, etc., but also assumptions about them, very harmful assumptions, and categories and labels, like people put into the NYPD's Gang Database without their knowledge. Those people in the NYPD's Gang Database are labeled as a gang member or an alleged gang member, and that label can follow them, right, in these data-sharing systems regardless of what they have or have not, and, as we know, many people in the NYPD's database were put there because of the color of shirt that they were wearing, the neighborhood, what they post on social media, so we also see that these labeling of people as criminal, as undocumented, as threats follows them and can further exacerbate those harms, and, again, we have very little regulation, transparency, oversight into these systems.

DANIEL SCHWARTZ: I think to just add on and something we haven't mentioned yet is also the linking of those technologies of databases of

correlating different technologies together is oftentimes greater than the sum of its parts, and I think a good example here is the Knightscope robot that was released or announced by the NYPD a couple weeks ago. That specific robot, or the deployment and pilot project did not follow the POST Act requirements to first post the use and impact policy, get public comment, and then finalize that policy before any procurement and deployment of such a technology, and this robot specifically, it combines video analytics, as mentioned earlier, it has video cameras, it has microphones, but also the vendor includes in its product facial recognition. Supposedly it's not being used, but it also includes other forms of video analytics such as license plate reader detection, it includes behavior detection, it includes signal detection such as when your phone pings looking for public wi-fi networks or known wi-fi networks, and combining all these technologies together is greater than the sum of like those technologies grouped individually because they allow for far greater insight and analytics capabilities, and that is also why we've been calling out the NYPD on separating out and/or (INAUDIBLE) also grouping

arbitrary technologies together in these ambiguous categories that they have created for POST Act disclosures.

CO-CHAIRPERSON WILLIAMS: Thank you. Are you able to share with us the different usages from private companies? Are they repackaging data? I know you mentioned the person who collected all of this data from Instagram images. How are they repackaging that data? Obviously, I'm sure they're selling the data, perhaps, but if you could just share a little bit more in detail how they're using the data and how they also might be repackaging the data when it's going to other parties?

ALLI FINN: It can work in various ways. I can speak to one example of data brokers and maybe someone else can speak more to Clearview, the company that you mentioned on facial recognition. Data brokers make their money by mass extraction, scraping, purchasing of our most intimate data, repackaging that data often with analytics products based on algorithms that can be biased to make predictions about risk, for example, and selling those to both private and government entities. For example, LexisNexis, which I am very much not a

lawyer, but legal students, journalists use LexisNexis research products, that's how many people know them, Lexis is a mass data broker and has been for decades, and they create dossiers on people. They advertise they have 10,000 or more public and private sources of data, 10,000 or more public and private sources of data, so they have these dossiers on people which include their biographic information, where they go, what they do, who they know, their health records perhaps, any court records, local tax and property records, utility data, marriage and divorce records, traffic violations, all of these comes into a usable profile that then only law enforcement can purchase including ICE and local police. That's just one example. I don't know if I answered your question.

CO-CHAIRPERSON WILLIAMS: No, that did. Thank you. How do you delete data out of these various systems? I know there's a lot of cyber security concerns if these systems are breached. Is there a way to extract your data outside of some of these systems?

ALBERT FOX CAHN: The terrifying reality is the vast majority of New Yorkers have no idea what

data is being collected by these systems to begin with. We have no way to confirm that it's being held, and we have no way, absent a court order, something that I've never really actually seen in these sorts of cases, that you could compel it to be deleted, whether you're looking at databases like the NYPD's Domain Awareness System or the government Fusion databases that share NYPD data with federal agencies like ICE, whether it's the private sector data brokers like Thompson Reuters and certainly LexisNexis. You can opt out of some systems. There are some cases in the private sector where you can, but in the public sector you can't, and, even worse, a lot of the time there are so many redundant copies of your data out there, by the time you opt out of one, they can just populate it from another database.

DANIEL SCHWARTZ: Just with regards to Clearview AI, for example, New Yorkers have no way of getting their biometric data deleted from that vendor. Residents of Illinois because of the BIPA law there have the possibility to get their biometric data deleted and also residents from Europe because of the GDPR protections.

CO-CHAIRPERSON WILLIAMS: Okay, thank you. Are there any ways that people can avoid being surveilled?

ALLI FINN: On an individual level, it is almost impossible, and that is why we need systemic action from the City Council. There's a lot of work there of how to protect yourself in a protest, for example, but it will never go all of the way. You'd have to opt out of 99 percent of society. That's an exaggeration, maybe, maybe not, so we strongly need action by the City Council to protect us on a societal level because individually this is so insidious and so unregulated that it's virtually impossible.

ALBERT FOX CAHN: I want to highlight that this isn't a fringe opinion. The United States Supreme Court, Chief Justice John Roberts even acknowledged this opinion in a case just a few years back where he said that these technologies are indispensable to modern life, you can't navigate the world without them, and so there is no effective way to opt out.

CO-CHAIRPERSON WILLIAMS: Yes, Nader in my office just gave me a quote earlier that if you want

security and freedom, you can't get both? What was the term? Tell me because it was a good term. Go on, say it.

NADER AHMED: (INAUDIBLE)

CO-CHAIRPERSON WILLIAMS: Yeah, so pretty much if you trade your freedom for security, you pretty much end up with neither, and so that's kind of what you're saying here, that, of course, people are trading in freedoms for the sense of security, but in trading in your freedom you essentially don't get either, like we're not more secure and at the same time and the same breath you're also trading off the freedoms that you have and rights to privacy.

ALBERT FOX CAHN: That's not a new position. Benjamin Franklin made that point more than two centuries ago.

CO-CHAIRPERSON WILLIAMS: It was Ben Franklin's point that he quoted to me.

Okay, do you have any suggestions outside of the bills today that the Council could consider to prevent companies from discriminating against people due to the usage of the technology?

ALBERT FOX CAHN: I think that in addition to the bills today it's really indispensable to have

a private right of action in both bills to ensure that individuals can have their day in court when their rights are violated. I think it's also crucial that we update the POST Act which was meant to require the NYPD to disclose these sorts of surveillance practices but which they have systematically violated for years, and now it's an opportunity to have greater accountability through legislation. I think we need to really revisit some of the decisions made on algorithmic discrimination a couple of years ago at the Council in the case of employment because New York law, we have a number of laws that have attempted to address the threat of algorithmic discrimination, but without actually having the sort of robust protections we need, and so really looking at outright bans on the most risky cases of algorithmic operations I think would go a long way.

CO-CHAIRPERSON WILLIAMS: I actually have a question on that because I know with the passing of that law that happened before my time companies are having a lot of conversations about copyright infringements, right, so if they have to be subject to an audit they are concerned that their proprietary

information, the algorithm that the company might've created to synthesize job applicants might now be subject to competitors because it'll suddenly be out in the open for the public so what is your opinion about that because that is an active conversation and it is my understanding that New York City is one of the first really government entities, I know in the UK, I know they've been looking at this, but in terms of like a government entity really seeking to regulate algorithms New York City is kind of the first out the gate and so what kind of recommendations or thoughts do you have around companies fearing that their proprietary information will now be out in the open for competitors to utilize?

ALBERT FOX CAHN: You can't have a robust financial audit without disclosing a lot of proprietary information. You have to open yourself up to scrutiny when you're going through a meaningful audit, and what I'm terrified of and what I warned the Council about several years ago as a reason not to pass the law is that we don't have any agreement about what an effective audit means and so it's like mandating a financial audit when you don't have

accounting rules, don't have a tax code, don't have any framework for how to do it, and so I think that for these audits to be worth the paper they're written on you have to have broad disclosure around training data, around methodology. It can't simply be a surface-level examination because that's going to rubberstamp a lot of systems that are augmenting discrimination.

CO-CHAIRPERSON WILLIAMS: Thank you. I have just a few more questions that I guess I'll ask on behalf of Council Member Gutiérrez.

The Administration mentioned at a blockchain hearing that they plan to provide digital wallets to residents. What are your comments, opinions about this announcement? What are the risks of having a digital wallet issued by the City and what are the risks of having digital wallets linked to biometrics?

DANIEL SCHWARTZ: I think we're really lacking details. There has been no announcement of this project. There has been little to no information of the scope, of the contracts, of the vendors, what the system would entail. I only know parts of the oral testimony that occurred, and I think it raises

privacy concerns, it raises security concerns, it raises concerns around really trying to influence shopping behavior made in that testimony, but I think we need more transparency and disclosure of what that project entails and what the guardrails.

With regards to the second part of your question, I don't think it's a place to deploy biometric identification there. We've seen in the instance of the IRS that had experimented with ID.me for biometric verification and the Department of Labor for unemployment benefits, the failure of using biometric verification because it was requiring people to enter their sensitive biometric information to get their rightful benefits, it was locking people out, accessibility issues, especially people with less tech literacy or access to devices or stable internet connection were struggling with getting their benefits or submitting their taxes and so I think there's a number of issues that could touch on that.

ALLI FINN: Yeah, I share these concerns and that we need to know a lot more. Some of my colleagues are working on this more than I am so also happy to follow up, but our understanding is that

some of these contracts were initiated through a demonstration project, I think I'm correct on that, not a more traditional procurement process that has points of additional oversight by different city agencies. That's how ShotSpotter came into use in New York City, also through a demonstration project to bypass some of those processes. It raises some concerns and red flags including some of the vendors involved. I agree about biometrics, and there is a long history of digital IDs and digital wallets which often sound convenient and sound like that increase sufficiency. The actual use cases often show that people end up getting denied access to rights and resources and they can become trackable tools that can increase discrimination. I'm speaking very broadly, but we would love to see the City Council investigate this further along with communities and organizers.

ALBERT FOX CAHN: Blockchain would be a boondoggle. It's an absurd proposition with no technical justification. We saw with the Excluded Worker Fund how bad some of these payment delivery systems could be using existing infrastructure, but to put every person's transaction on the blockchain

would make meaningful privacy protections impossible, and it also would just be a security nightmare. To me, it honestly felt like just buzzword bingo and not serious policy.

CO-CHAIRPERSON WILLIAMS: Thank you. I don't think anyone else has any questions so I'll turn it back to you.

COMMITTEE COUNSEL BYHOVSKY: Thank you. I want to thank the panelists for your testimony, and we're going to move to our next panel.

I would like to welcome Lisa Meehan, Robert Tappan, sorry I mispronounced it, and Hally Thornton to testify.

Any order is fine.

LISA MEEHAN: Can you hear me? Okay, it's working. Hello. My name is Lisa Meehan. I'm here to testify on behalf of Mobilization for Justice.

Mobilization for Justice offers free legal assistance to low-income New Yorkers in many areas including housing law. We work alongside tenants and community-based organizations to prevent evictions, obtain repairs, and protect tenants' rights, and we appreciate the opportunity to share

with the Committee our thoughts on limiting the use of biometric recognition technology.

It is well-documented that facial recognition technology is less accurate at identifying the faces of people of color, women, elderly people, children, and transgender and nonbinary individuals than it is at identifying the faces of cisgender white men. As a result, tenants are often misidentified by the technology in their buildings. Tenants at one building have to resort to humiliating dances in front of their cameras just to be seen by the cameras, and guards end up buzzing in everybody who is waiting. The cameras at that same building mistakenly let a tenant's cousin in even though the tenant's cousin did not actually live in the buildings so, overall, both false positive and false negative matches result in less security for tenants rather than more security. Even if the technology were able to identify all faces with perfect accuracy, its use is still a violation of tenants' privacy. It infringes upon our most basic fundamental rights to privacy and freedom of association under the First Amendment of the Constitution by putting up barriers for tenants who

want to invite guests, family members, or service workers like home health aides to their homes. Landlords also use technology to surveil and harass tenants, particularly tenants who are already marginalized and at increased risk of being displaced. Lastly, the technology is dehumanizing. As one tenant said, we do not want to be tagged like animals. We are not animals. We should be able to freely come in and out of our development without our every movement being tracked.

In conclusion, Mobilization for Justice urges the City Council to pass the initiatives and protect New York City residents. Thank you.

CO-CHAIRPERSON WILLIAMS: Thank you.

ROBERT TAPPAN: Thank you. Good afternoon, Council Members, Chairman Gutiérrez, Chair Williams. Thank you for giving me the opportunity to address you today.

My name is Rob Tappan. I am the Managing Director of the International Biometrics and Identity Association based in Washington, D.C. We are a non-profit industry associated charted to advance the adoption and responsible use of technologies for managing human identity and to enhance security,

privacy, productivity, and convenience for individuals, organizations, and governments. We do this through advocacy, engagement, and education.

Our reason for appearing before you here today is to communicate our concerns to the Council about the potential for overreach and the unintended consequences in the proposed draft legislation in bills 1014 and 1024.

With regard to the proposed language contained in bill 1014, I would tell you that residential building security is only as good as the weakest component, which is usually humans. The principles of various assurance levels of physical and logical security using multifactor authentication are well-captured in documents and standards published by the National Institute of Standards and Technology or NIST. The highest levels of assurance include biometrics as authentication factors. For building trying to offer highly secure environments for their tenants and residents, all residents and guests should be required to enroll biometrically or that high level of security can’t be guaranteed. We do this in our businesses and our enterprises as well as in hospitals and healthcare facilities, and

building owners should be allowed to offer this level of security to their tenants. This level of security isn't a threat to be restricted. Rather, it is a privacy- and security-enhancing feature for residents and their guests. In the broader commercial space, biometric technologies are useful in fighting crime and reducing theft. The ability for stores, shops, and merchants to prevent shoplifting and robberies, or at least hold perpetrators accountable, is key to controlling this worrisome trend. According to a recent article in the New York Times, over the past five years shoplifting complaints nearly doubled, peaking at nearly 64,000 last year police data shows. Only about 34 percent resulted in arrests last year compared with 60 percent in 2017. Biometric technologies help in reducing crime, identifying repeat perpetrators as well as facilitating loss prevention and, when stores can't control their losses over time, they must make a difficult decision about to whether they remain in business in that location or their neighborhood. I have just two more sentences. When stores and commerce flee that area, that can create phenomena like food deserts limiting the options of area residents which in turn

exacerbates the cycle of crime and economic despair. Asking criminals for permission to enroll them biometrically isn't realistic and doesn't support the objective of reducing crime in New York City. I'll leave the rest of my remarks for the record please. Thank you.

CO-CHAIRPERSON WILLIAMS: Thank you. Council Member Holden.

COUNCIL MEMBER HOLDEN: Thank you both for your testimony. I'll ask you both. What you said is that if the residents opt in for facial recognition, is there anything wrong with that, that the residents said I wish to participate in this because my building would be safer, would you be against that? Let me ask, because you spoke against it, would you be against that?

LISA MEEHAN: Our concern with opting into the technology is that oftentimes tenants wouldn't actually get the option to opt in. That option wouldn't actually be communicated to them by their landlords, and then, even if they are given the choice to opt in, oftentimes tenants wouldn't feel like they actually had a choice because of the power

imbalance between landlords and tenants so we would have an issue with that.

COUNCIL MEMBER HOLDEN: Let's say there was a bill, or included in this bill, that residents could opt out of the bill because they would like to have their building, whether it's their perception or not whether it's safer, but that they feel that they want to keep people who are constantly getting in the building, let's say the doorman or security person misses the person going in and gets in the building or somebody brings somebody in that had domestic violence, let's say, issues, and we want to keep them out, technology often is better than somebody saying I think that person looked like that guy, I'm not sure, whereas the biometric, I've read issues and maybe you could attest to this, but that what you had mentioned in your testimony that mostly people of color are singled out in this, that the technology was bad, that was the case, but the articles I read, that was the case years ago but not anymore, and what I'm reading is there's a 95 percent success rate. Do you have any other information on that, on facial recognition?

ROBERT TAPPAN: Yes, Council Member. Yes, the cycle of innovation that has taken place even since 2019 where this sort of misnomer first occurred, the development of technology and innovation has quintupled, grown at an exponential pace in order to improve and be better and more effective and more accurate.

COUNCIL MEMBER HOLDEN: Have you heard the 95? Because I've read articles where it said 99 percent success rate, 95, that's not good enough? People opting in and say my building, I live in this building because I'm afraid and I'm afraid of who gets in the building, I don't believe that security at the desk is good enough, or whatever the reason, if somebody wants to opt in, shouldn't they be able to? You say yes, but you say it could be slipper slope I guess, right?

ROBERT TAPPAN: Council Member, I just want to make one point, and it's a personal story. I have two parents in assisted living right now. They're in a folks home not too far from my house. Every time I go and visit them, I go to a kiosk, type in the person I want to see, my mom and dad, and I go through a facial recognition thing because I

preregistered, I gave them my driver's license, they've compared it to my face, and it lets me in, and I want to be let in to see my parents, but I don't want some stranger off the street and neither do any of the other sons and daughters of members at an assisted care facility want that so it is truly a very good security measure and keeps places safe and secure.

COUNCIL MEMBER HOLDEN: Thank you. Thank you, Chairs.

CO-CHAIRPERSON GUTIERREZ: Can I ask you a question? Can you share examples of incidents where landlords adequately informed their tenants about no hot water, about a broken elevator, no heat? I think it is wildly irresponsible to position landlords to put up notification in their buildings about opting out, it is really dangerous, because they don't even do the minimum to meet dignified housing in many cases and in Districts like mine. I don't know about every other District that maybe has privilege to have doormen, but that doesn't happen in a lot of communities of color so do you have examples of when that does happen?

LISA MEEHAN: Not on top of mind. I can't think of any specific examples of landlords providing notice for things like that, no.

CO-CHAIRPERSON GUTIERREZ: So would it be safe to say that you also don't feel confident that they would even follow the existing law which is notifying tenants of when their biometric information is being captured now?

LISA MEEHAN: Like we said, our concern with opting out or even opting in is that tenants often don't feel like they have a choice when they're in negotiations with their landlords because of the power difference between landlords and tenants in these types of negotiations, and there's the troubling trend of technology, any kind of technology used by landlords to surveil and harass tenants. In our written testimony, we talked about a lot of examples that are well-publicized of landlords using, for example, typical security cameras without facial recognition technology to harass tenant organizers, to screenshot minor lease violations and try and evict tenants.

CO-CHAIRPERSON GUTIERREZ: Thank you.

ROBERT TAPPAN: Madam Chair, may I respond to that as well very briefly? One of the things that I've seen at this hearing today very ably run by you and your Colleagues here by many of the respondents is that there's a conflation of terms here. Sometimes we're talking about surveillance in the strict sense of the word when we're actually talking about verification or authentication. When we're talking about the use of biometric information versus what a dumb closed circuit television camera that's actually recording video, there's a little bit of conflation between these two types of things. Biometric technology has so much more computer power and analysis behind it than closed circuit television in the same way that having a smart card to buzz you into your apartment, it might record some information but it doesn't record your biometric information so there's, I think, a conflation of some of these technologies where we might hate the fact that when we use our keycard that our landlord or the apartment building owner knows that we come in at 11 o'clock at night and we don't leave until 11:30 the next day, we don't want people knowing that information but that has absolutely nothing to do with biometrics. That

has everything to do with technology making sure that the people who are where they need to be and are allowed to be there are allowed to get in, and it's the same way with biometrics in that if you want access to your account and you can use voice recognition in order to be verified, that's something that her voice is not the same as my voice, and if I'm trying to access her bank account, my voice ain't going to make it but hers will, and the integrity of that, the integrity of that biometric technology behind it is really what the security is all about.

CO-CHAIRPERSON GUTIERREZ: I appreciate your response. I understand that distinction. I'm speaking specifically about how biometric data is used and can be abused by landlords, specifically in buildings with predominantly people of color and the ease of which, the Administration here, I think, identified how they're not really working or have no sense of whether existing laws are even being enforced, right? We walked into this hearing, hearing from them that there is no indication that they can share, yes, this Local Law is being enforced. We heard from advocates the opposite. What I'm saying is that it is far easier for landlords in these

situations to potentially abuse that and not solely use it for the purpose of security or safety for their buildings. They can utilize it, and there are examples of them utilizing that to evict tenants, to give that information to PD, and in those instances every time that data is shared, that person's biometric information is being compromised because they're being added to lists that they're not even aware of, and that's what I'm trying to drive home, the abuse of that. I get what you're saying. Council Member Williams.

CO-CHAIRPERSON WILLIAMS: If you can share, you mentioned integrity, if you can talk a little bit more about I guess companies that are members of your non-profit association, the industry association, if you could share how they maintain integrity because I hear what you're saying, and it makes sense. If you need to scan a fingerprint to get into a building, that's completely different from having other information that could be calculated from the single use of your fingerprint to get into the building, but how can companies sort of safeguard against that because I always say it's not necessarily the technology, it's who is using the

technology, and what the technology is being used for and because oftentimes in government we can't regulate it, it just becomes dangerous across the board so how do your members sort of protect and safeguard against integrity?

ROBERT TAPPAN: All very, very good points, and I agree with you on many of them. If you put a good technology into bad hands, something bad can be done with it, and you can put a person behind a car and they get a place to drive to work every day, but you can also put a bad person behind a wheel and they kill somebody so the technology is Switzerland, it is dependent upon the user and the usage. Our members have agreed to a code of ethics, a code of standards of ethical conduct and responsible use of biometric technologies. It's all on our website at ibia.org so those sort of principles can be looked up and our members adhere to them. A large part of our membership does business with the federal government and state and local governments around the country so our members are part of programs that are administered by the Department of Homeland Security, the Transportation Security Agency, the Customs and Border Protection, as well as any one of a number of

law enforcement entities out there, and the usage for this is security, identification and verification, and, in the milieu of travel, it's to assure that the people who have a boarding pass or use their face as a biometric in order to get on the plane are the people who they say they and that are the people that are supposed to be on that plane or getting on and off a ship at a port of entry and exit and coming into the country. We have biometric passports, and we have biometric cameras at our entries, CLEAR program, any one of a number of a different programs that use biometrics. There was a question that's been asked a number of times, what are the good things about biometrics, what good aspects of biometrics are there, and there's many, and I can go off the shores of the United States and go to India where the AADHAR national ID program is being implemented right now. Right now, there are 1.6 billion people who are now able to have an ID that they can show and get benefits from the government when they couldn't do it before because they had no identity before that. There are just any one of a number of Indian faces, right, so you've got this identity card now. That gives you something. That's currency. That is

existence. That is identity. It's those sorts of things that really are the positive parts of biometrics.

CO-CHAIRPERSON WILLIAMS: Just another question in the same vein. Outside of integrity, I know that there's been a lot of conversations around the makers of various algorithms and how information is scrubbed so if you have someone creating an algorithm, a human creating an algorithm or plugging into a computer, you know humans, we all have bias, every human has a bias…

ROBERT TAPPAN: Absolutely.

CO-CHAIRPERSON WILLIAMS: Have your member organizations, do they look at that type of…

ROBERT TAPPAN: Indeed, they do. I'll make two points about this. One, to answer your last question first. They look at that time all the time. NIST, the National Institute of Standards and Technology, does a competition every year with the largest makers, actually any company that develops algorithms and these types of technologies can enter, and it goes to the old adage garbage in, garbage out. The 2019 NIST study made some generalities about some really bad algorithms that were out there and that

was maybe first, second generation, and really don't reflect the algorithms that are here right now, and that's the pace of innovation and the pace over five years. The other thing about algorithms, and I like to use analogies and I'm not trying to dumb this down at all, but an algorithm is like a recipe. You have a recipe for brownies, and you know that you have to bake them at 350 and you add an egg and you add some oil or butter and 25 minutes later you have brownies, right? Some people like chewy brownies and some people like cakey brownies, right? Add more eggs, you get cakey brownies. You add more fat, you get chewy fudgy brownies, right? These algorithms can be manipulated and they have been, right, but it's not in the best interest of any good upstanding company who is in the biometrics industry, that has any ounce of integrity, to build in white bias or majority bias, it doesn't make any sense. You're striving for perfection. You're striving for, okay, the word discrimination has two meanings, right. Discrimination is the bad one, the first one is discriminating against people and sidelining them. The one about discriminating is actually coming to a finer point and getting to the accuracy of something.

You're discerning. You've got a discriminating palate. That's what our member companies are trying to do with the algorithms that they are building. They're trying to get more and more accurate, and the Council Member who did say that there was 95 percent accuracy on some, indeed there was in the last set of NIST tests. Is there ever going to be perfection? No, but we can strive for perfection, and that's what our member companies try to do. Thank you.

CO-CHAIRPERSON WILLIAMS: Yeah. How are they controlling for that? The explanation that you provided, do you know how they're controlling for that, how are they trying to get to better accuracy, how are they running test models, maybe even brining different people into the company, what are the tangible things that they're doing to control for said potential bias that might show up in these various systems?

ROBERT TAPPAN: Yes. Thank you for the question. First of all, I'm not a true technologist. Otherwise, I'd be working for a biometrics company myself. I will say that a lot of this has to do with the datasets. In the early days of coming up algorithms, there was a control set that probably was

predominantly white, Caucasian, light-skinned, right? Over time, we've been able to absorb more and more datasets of people of various shades of skin color, etc. That makes the algorithms with each iteration become more and more accurate so it's a matter of ongoing testing, ongoing innovation, and expanding the universe of people that are in that dataset.

CO-CHAIRPERSON WILLIAMS: Outside of the datasets, are there any like focus groups that some of your membership organizations have or like special committees just to get sort of that, because one of the things that the Chief Privacy Officer talked about is independent reviews and he also talked about transparency so one, providing information to the public in terms of what the algorithm is, what the data is showing, but then he also said, I wrote it down somewhere on one of these papers, I wrote on a thousand papers today, I don't know why, that was very, very silly of me, it might be under here…

ROBERT TAPPAN: Ma'am, to your point there are professional associations like myself, IBIA, and then there's also the Security Industry Association, there's any one of a number of industry associations that gather scholars and technologists of all

different backgrounds in order to be able to make things like algorithms more accurate and that sort of thing. NIST is also involved. I look at this as a big partnership. We've been asked and actually cooperated just a few weeks ago with the National Academies of Science, Engineering, and Medicine and provided our testimony into how our membership is making algorithms more accurate, less biased, and more focused on getting towards that 100 percent accuracy, and so there is a very large network of government, private sector, trade association, and then enterprises who are actually in the business who are all cooperating together. Is it perfect? Is it at the urgent pace that perhaps this Council is looking for? I don't know. That remains to be seen, but I will tell you that it is being worked and that we are dedicated towards making it better so that we don't have to appear before you all in this sort of adverse situation.

CO-CHAIRPERSON WILLIAMS: Yeah. I think he said independent evaluations so just was wondering if…

ROBERT TAPPAN: I would consider the National Institute of Standards and Technology to be

an independent body. Though funded by the federal government, it certainly has a stake in the way that the FDA has a state in making sure that drugs are safe and efficacious.

CO-CHAIRPERSON WILLIAMS: Thank you. I think that's all. Thank you.

COMMITTEE COUNSEL BYHOVSKY: I would like to thank all panelists for their testimony, and we're moving to our next panel.

I would like to welcome our last panel in-person, and then we will call witnesses who are here virtually.

Our next panelists are Jake Parker, Jay Peltz, Stuart Reid, and Francisco Marte.

JAKE PARKER: My name is Jake Parker. I'm with the Security Industry Association, a non-profit organization representing more than 70 companies headquartered in New York. I appreciate the opportunity to participate and be before you today.

Our members provide a broad range of security and life safety products and services in the U.S. and throughout the City including biometrics. Today, biometric technologies contribute to the safety and security of our communities and bring

value to our daily lives. In nearly all cases, businesses are utilizing this technology as a better way to accomplish pre-existing underlying processes of verification and identification that is already occurring through other less effective means. The purposes generally fall into two categories, enhancing business operations and also optimizing the functionality or security of products and services used by customers. The vast majority of these applications are opt-in and based on prior consumer consent.

We do have some concerns about the two proposals before us today. I think a measured approach could address some very specific concerns about the technology, and we understand that there are concerns, but the measures would simply outlaw most uses of biometric technologies by businesses, consumers, and property owners regardless of the type of biometric, regardless of the purpose, and regardless of whether it’s a service that’s been requested or agreed to by an individual. This would rob consumers of the choice to use more secure and convenient methods to verify their identity, and it would dictate unnecessary limitations on methods New

Yorkers can use to protect themselves and their property. No other jurisdiction in the U.S. has ever considered something of this scope.

Here are just a few examples of the biometric technologies that would be eliminated under this type of prohibition. Customer choice of biometrics is a more convenient form of payment and access at sporting events and entertainment venues, biometrically secure driver authentication for rideshare services, fingerprint access for gym members, use of increasingly popular virtual doorman systems by homeowners' associations and residential buildings which offer a more secure and convenient access for residents, we've talked a bit about this today, use of fingerprint timeclocks and cash register locks by business and employees, biometrically secure building and door access systems for workers, biometrically enabled security systems protecting persons or properties including systems that augment efforts to fight organized retail crime and address the theft issue that we certainly have (INAUDIBLE) systems have been able to greatly reduce incidents of theft. Also use of biometrics for streamlined embarkation by airlines and cruise lines

providing curb-to-gate travel services. Earlier on, it did come up the question about airlines and travel services, I don't see any kind of exemption in this draft that would make these restrictions not apply in those instances to the services we were talking about unless I'm missing something.

I'll just say one last thing, there is an existing biometric data law in place in the City which is unique and one of its kind which has just recently gone into effect 18 months ago, also the Tenant Data Protection Law has just gone into effect in January and requires consent for biometric use in those types of systems, and it covers electronic access information so I think we should see how the regulations goes before layering on further prohibitions.

JAY PELTZ: Good evening. My name is Jay Peltz, and I am the General Counsel and Senior VP of Government Relations for the Food Industry Alliance of New York. FIA advocates on behalf of grocery, drug, and convenience stores throughout the state. We represent a broad spectrum of the NYC retail food sector from independent neighborhood groceries to large chains including many unionized stores.

We oppose this legislation because it not only bans the use of biometric recognition technology to identify a customer without a public safety exception, but it also creates numerous new conditions on the collection of biometric identifier information that are so far-reaching that they effectively prohibit the accumulation of such information by the City's grocers. The inability to collect such information and use biometric recognition technology would seriously undermine the ability of the City's grocers to deter shoplifting and assist law enforcement investigations of repeat offenders. The failure to reverse rising thefts at marginal grocery stores will likely result in the closure of those locations, thus exacerbating the City's food desert problem. Historical NYC crime data demonstrates a recent surge in petit larceny complaints including a 46 percent increase in such complaints between 2020 and 2022. A rise in retail theft is accompanied by an increase in threats of violence and actual violence during the commission of such crimes. This creates the need for merchants, many of whom are people of color, to use legal ethical methods that are nonconfrontational to deter

theft and assist law enforcement investigations of repeat offenders. Biometric systems are focused on identifying recidivists who commit a disproportionate share of thefts in the city. It is our understanding that the commercial use of facial recognition is legal in all 50 states. In addition, there's a current trend away from blanket bans of facial recognition technology. The trend towards expanded facial recognition includes appropriate privacy protections and exemptions for safety and security applications. This is why we oppose this legislation and strongly support a collaborative effort to replace this bill with a new measure that will allow the collection of biometric identifier information and its use through biometric recognition technology that enables the identification of individuals for the well-being and safety of customers and workers.

We look forward to participating in such a cooperative process with Council Members and other government stakeholders. I'd be happy to answer any questions you might have.

FRANCISCO MARTE: My name is Francisco Marte. I didn't bring nothing in writing because it was short notice and, besides that, because I'm going

to tell the (INAUDIBLE) and the facts. I am really opposed to this draft.

Since 2020, we've been facing a lot of problems (INAUDIBLE) bodegas and supermarkets. I'm talking on behalf of the bodegas (INAUDIBLE) small businesses, restaurants and (INAUDIBLE) as well as supermarkets. We've been having a lot of problems. Now the technology is helping us. This type of technology is to prevent a crime to happen and how we can prevent, in a small (INAUDIBLE) to be turned into (INAUDIBLE) use these technologies, we will prevent a lot of problems, a lot of incidents that happen. We will keep using this. Even we put a sign outside saying that we are using the recognition technologies in the store that we are using. As the President of Bodegas and Small Business Association, I've been promoting to my members that you have to use it because we need to product our customers, our employees, and our business. We've (INAUDIBLE) a lot of problems (INAUDIBLE) a lot of problems that happen because of the violence so this wave of violence was created since 2020 when (INAUDIBLE) start to disrespect the police, when the Police Department lost their respect so it's a (INAUDIBLE) that right

now the sponsor of these bills, in their Districts there are high crimes, and we, the business community, we've been suffering a lot as the working-class (INAUDIBLE) I hope that if this bill passes, the Mayor vetoes them because we will keep fighting even we have to move to another (INAUDIBLE) because we will keep using this to protect our business, our customer, our community. That was that, but I just want to make this very clear. These don't (INAUDIBLE) no one because when we use (INAUDIBLE) if someone comes, a repeat shoplifter or a criminal comes, he is just going to get a notice. We don't deny anyone to come, even if you are already an offender. What we do is we keep eyes on you to prevent that you commit a crime. That's what we do. These technologies are really helping the store owners and the communities (INAUDIBLE) Thank you.

STUART REID: Good afternoon, Members of the New York City Council on Technology, Chairs Gutiérrez and Williams, guests gathered here today. Thank you for giving me the opportunity to speak about technology, security, and safety in New York City. My name is Stuart Reid. I'm the Co-Chairman of The Smart Community Initiative, TSCI, a 501(c)(3)

not-for-profit partnership of public housing and residents and veteran New York City community technologists who have come together to help improve the quality of life for our residents utilizing innovative technology applications and services.

While TSCI certainly applauds the Council's efforts to reign in and regulate the use of technology to monitor and surveil in the name of public safety, particularly with the accelerated implementation of AI, TSCI encourages the Council to also invest its attention and resources to support successful community-based public safety initiatives utilizing innovating technology to keep our public housing developments safe. TSCI believes that our communities themselves should be in control of our own public safety and security rather than some third-party technologist, agency, or government entity. TSCI and its Directors have been working in partnership with public housing residents for decades on this very issue. TSCI trains residents in emergency and public safety communications, procedures, and protocols utilizing mobile radios, smart phones, and other communication devices to stay in touch with each other and to keep our communities

informed. Working in collaboration with resident association leadership, TSCI installs emergency digital bulletin boards in building lobbies that display and announce emergency preparedness and mitigation information as well as development news and information. TSCI also works with residents in creating the Virtual Tenant Patrol Service which enables residents to view live images of their building's lobbies, entrances, and other public spaces on mobile phones and connected devices. Where residents, many of them seniors, previously sat in building lobbies to monitor and report on suspicious traffic in their buildings, they are now able to do so remotely without sitting directly in what could be harm's way. The emergency digital board and Virtual Tenant Patrol services put public safety and quality of life directly into the hands of residents. The service is completely controlled by resident leadership, including programming of emergency and building announcements and also serving as an information kiosk. When everyone can see what's going on in the development, when everyone is informed and aware of their building conditions, threats, and safety protocols and responses, the community,

itself, becomes its own watchdog and first responder as we all work together to keep each other safe.

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

CO-CHAIRPERSON GUTIERREZ: Thank you. I have some questions for both Francisco and Jay. Curious in both of your experiences, your members, what specifically is being captured by the biometric collection?

JAY PELTZ: Right. With our members, it's just facial recognition. No other metadata. No other personal identifier information. If there's a match, it's a better system than the old school dumb systems because if there's…

CO-CHAIRPERSON GUTIERREZ: Which is just a security camera, do you mean?

JAY PELTZ: Well, it's not smart.

CO-CHAIRPERSON GUTIERREZ: Okay.

JAY PELTZ: There's no app. It's not software based. It's better because it's faster and more efficient and a lot more accurate. Much less chance of error. If somebody is observed committing a crime in the store, then an image is taken and stored and, if there's a hit on that image again when that person comes in, then internally to the loss prevention people there will be a message sent if there's a match.

CO-CHAIRPERSON GUTIERREZ: I see.

JAY PELTZ: And then the store is in a position to assist law enforcement if law enforcement is interested, which they aren't always interested, but that's all that's done with it. It's just a tool that can assist law enforcement in their effort to enforce the law. The problem historically with shoplifting cases is that the police simply didn't have enough evidence to go on so shoplifting historically has been under-enforced. I've been around the business since I was born. My dad was in the business, operated independent grocery stores in the stores. I operated independent grocery stores. It's been very difficult to prosecute those types of cases because of a lack of evidence. These systems

create the possibility of having accurate eviction which is a match on somebody's face.

CO-CHAIRPERSON GUTIERREZ: Before you answer, just one followup question for you. In those instances, I appreciate the timeline because that was going to be my followup question. In those instances where there is a capture of some theft happening and then the next time the person comes in, do you have a sense of how often does that happen? Our concern is, yes, the biases of algorithms but also the fact that like technology is not perfect and kind of the risk that that could put people in so do you have a risk of like how often that happens where it's capturing the right person or kind of what that discrepancy looks like?

JAY PELTZ: My understanding, what's being reported to me is that the system is very reliable, the error rate is very low, but the number of incidents overall citywide are up. In 2022, there were over 115,000 complaints according to the NYPD of petit larceny. That's the highest number by far throughout the 2000-2022 period, but theft rates vary by individual store, individual neighborhood.

CO-CHAIRPERSON GUTIERREZ: Okay. Francisco, for your members (INAUDIBLE) supermarkets?

FRANCISCO MARTE: Yes.

CO-CHAIRPERSON GUTIERREZ: What is the data that they're collecting and walk me through similarly if you can the way Jay did like how does that prevent theft for the business owner?

FRANCISCO MARTE: Yes. Similarly like he said, we just collect the image, and it's just to prevent, when the people, we don't deny the service (INAUDIBLE) knows that we know that they're there so if you come to commit a crime, don't do it. Just leave. If you're not going to shop, you're not going to buy, just go. Don't try to shoplift because we have the eyes on you, and that's better because that's a prevention so basically this camera has already doing for us (INAUDIBLE) to prevent for a crime to happen or a violence because of shoplifting.

CO-CHAIRPERSON GUTIERREZ: In the occurrence where the person who maybe previously committed theft comes back, doesn't do anything, what happens there after that match is made?

FRANCISCO MARTE: If they don't come?

CO-CHAIRPERSON GUTIERREZ: No, if they do come but they don't do anything. They maybe patron the store.

FRANCISCO MARTE: All right. Yes, if they don't commit a crime, we won't do anything to them.

CO-CHAIRPERSON GUTIERREZ: Will it still go (INAUDIBLE)

FRANCISCO MARTE: (INAUDIBLE) is going on.

CO-CHAIRPERSON GUTIERREZ: There's still notification and so that happens and so now you're just watching this person more carefully?

JAY PELTZ: A person can be barred from a store. It's a private establishment. If a person is witnessed shoplifting a number of times, that person might be barred, a letter sent to the local precinct. If that person has been barred, then, at the discretion of the store, they can contact the local precinct and then it's up to law enforcement to take it from there, but there are a couple of points I wanted to make related to your overall line of questioning. This is all about somebody, one of the panels before talked about stealing a bottle of beer. We're not here because people are stealing individual bottles of beer. We're here because of repeat

offenders. In my full testimony, there's a reference to a New York Times article that about 1/3 of shoplifters, about 327, have been arrested and re-arrested 6,000 times, and the issue now for the first time in my life going back to 1963, that organized retail theft is hitting grocery stores so they're causing thousands upon thousands of dollars' worth of damage, and what our members are trying to do is to address that problem. That's where the focus is.

In terms of bias, first of all, we represent chains and independents. Most of our independents probably are people of color, Hispanic people, Arab people. They're not biased against people of color, and they're not going to allow it to happen if…

CO-CHAIRPERSON GUTIERREZ: Oh, they are, speaking from my community, but go on. Everyone is biased.

JAY PELTZ: In our experience, bias is profoundly offensive. It's a complete waste of the owners' resources. They're not investing in the system in order to give people a hard time who aren't committing any crimes in their stores. If they're deemed to be engaged in bias, it's likely to result

in loss of business so bias is not something that our owners are interested in nor is it something that they would allow to continue so if the return isn't there, the return is measured solely by how many repeat offenders do you catch, they're going to shut the system down.

CO-CHAIRPERSON GUTIERREZ: For both of your membership organizations, was the use of biometric technology installed during the pandemic, 2020? Just because I understand what you're saying, your concerns, I believe there's like a bigger issue around why people are stealing food or grocery stores for example, but I'm just trying to…

JAY PELTZ: Well, people steal food for different reasons for sure, but the big problem is the organized retail theft rings who have their own warehouses, it's like product in, product out, they're making a fortune. That's got nothing to do with people starving and everything to do with people who want to make money through illicit means. My understanding is that our members have increased their purchase of these systems since 2020 when state level reforms were enacted and crime rates went up, theft rates went up as a response to that.

CO-CHAIRPERSON GUTIERREZ: You're referring to bail reform?

JAY PELTZ: I'm sorry?

CO-CHAIRPERSON GUTIERREZ: You're referring to bail reform?

JAY PELTZ: And other measures that were enacted by the State.

CO-CHAIRPERSON GUTIERREZ: Okay. Francisco.

FRANCISCO MARTE: We've been having this problem, the problem started to get worse since 2020, but we already had been having that kind of problem but we didn't have the technologies and while we are using the technology just to prevent, that's what we are doing, it is a prevention (INAUDIBLE) we've been resolving with the facial recognition. Like I told you, we don't collect data, we don't share that information, it's just for us, to protect us, from the shoplifting. Remember, over 97 percent of the people who do shoplifting, they do it to resell or to use drugs or do something. They don't do it for need. In New York, we are not in that situation, the hungry, because there's so many pantries, there is food everywhere. If they came to any of our stores

and they ask for food because they're hungry, we are going to give them food. It doesn't matter, you know, we don't ask if you are, how can I say, for a (INAUDIBLE) or nothing like that because, like he said, we are independent owners, we work hard and we have to defend our stores because that's the only (INAUDIBLE) we have.

CO-CHAIRPERSON GUTIERREZ: Thank you.

CO-CHAIRPERSON WILLIAMS: I just had a comment and then I guess a question.

The comment, I just wanted to mention that I know you, Mr. Jake, you mentioned some of the beneficial applications that would be eliminated and some of them would not apply to this law, but some of them, you are right, would apply to the law. I just wanted to mention that to you, that some of them would be exempt from having to comply with this law because they're specific to public accommodations and the other one is specific to housing.

The other thing I wanted to ask in that same vein is would you be, or any of you all since you all oppose the bills, would you be open to amendments to the public accommodations bill that allows for people to consent to have their biometric

information used to verify and/or identify them? Would you be okay if that was included, because I know that's technically not included in the bill. It's just a consent to collect information, but the bill will still ban all forms of biometric identification to verify and/or identify a person so would you be okay with the bill if that amendment was made?

JAKE PARKER: A couple of problems there. One is that for the security and safety type of applications that we're talking about, consent really isn't appropriate and that would not work for the functionality of those systems. Certainly, notice is important. I think that can be provided in a lot of instances. Also, then it becomes a concern about the method of enforcement through the private right of action where we've seen in other jurisdictions, in primarily Illinois, where technical allegations about whether consent has been provided or not can be the basis of frivolous lawsuits and can really damage particularly small businesses in that state that have been sued in the instances where no harm to a person has occurred but there's an allegation of a technical violation so I think that concept should work but

there needs to be reasonable exceptions for safety and security.

CO-CHAIRPERSON WILLIAMS: I know in Texas they ban, and I'm trying to pull it up, but they don't allow for the private right of action that you mentioned. It's only the Attorney General that can enforce the violations of the law so what is your opinion about the Texas version?

JAKE PARKER: That's a state level law. It's really a different situation. What the Council has already passed, the Biometric Data Ordinance in 2020 I believe it was and the Tenant Privacy Act from 2021 that has just gone into effect, both include a private right of action as the enforcement mechanism and so I definitely think there could be abuse of that mechanism. We haven't seen, I believe, but maybe just one lawsuit so far under the Biometric Data Law, but certainly a concern.

CO-CHAIRPERSON WILLIAMS: I know it's a state law. I was just wondering how you felt about removing the private right of action and creating more of a government entity that can enforce because there have been bills that particularly have come before my Committee and, of course, the concern is it

opens up companies to a whole bunch of lawsuits and so if there was a way to, I don't know, perhaps minimize that, would you be in support of the legislation?

JAKE PARKER: I think as a general statement that's a better way of enforcing laws like this, but I think in this case I think the question why haven't there been more lawsuits if the level of abuse is what it's assumed to be.

STUART REID: I would just like to mention, Council Member Williams, I do not oppose the bill, TSCI does not oppose the bill, so though I'm here with these other gentlemen that do, you mentioned "you all," I'm not among that group, and I also just wanted to say that one of the earlier panelists talked about the power equation of who is in control of the technology, who's in control of the cameras, who's in control of the data, and I think that is so important, and what our experience has been, TSCI's experience has been, is when the people on the ground, when the residents are in control of the technology and the data, it changes everything. It becomes no longer a punitive technology. It becomes more of a preventative technology, and I

think that's something that I encourage the Council to explore further.

CO-CHAIRPERSON WILLIAMS: Thank you for the clarification.

JAY PELTZ: If I may. Regarding private right of action, one of the problems with private right of action clauses in the city is that I've never seen one with a provision that allows an establishment to allege that the claim is frivolous. Our members face way too many lawsuits as is, many of them are frivolous, and that's the worry is that there will be more frivolous lawsuits.

In terms of consent, that wouldn't work for the grocery sector because there are thousands of transactions, thousands of customers that go through grocery stores, each store, in any given year so you can't possibly get consent from a significant number of them. There's the likelihood of litigating over whether or not the consent was properly given or the underlying validity of the consent. The big problem is that wrongdoers, particularly members of organized retail theft rings, are not going to consent to their information being collected or to a system being used to apply that information to identify them.

CO-CHAIRPERSON WILLIAMS: Okay, I know consent is one thing, but what about a public notice? That would work for a supermarket.

JAY PELTZ: Public notice in the current law? Yeah.

CO-CHAIRPERSON WILLIAMS: No. I'm just asking your opinions about different potential tweaks because you're opposing the bill so I'm just saying would you like if it had this, would you like it if it had that. You said consent wouldn't work because I get it, you have to like sign and say I consent to this, but you can't do that when you're walking into a supermarket so what I'm saying is what about a public notice?

JAY PELTZ: We would be open to a reasonable public notice requirement, sure.

CO-CHAIRPERSON WILLIAMS: Okay. Thank you. Council Member Holden.

COUNCIL MEMBER HOLDEN: Thank you again. I have a, I guess most of us do in New York City, we have the retail drug chains that have locked everything up behind plastic covers and cabinets and you need a key because we've never seen anything like this where people walk in with plastic bags and the

same people are walking into these establishments, Chairs, the same people are walking into these establishments with a bag and they fill it up. That's why the drug chains have done this. They've made it an inconvenience to go and shop because you can't get toothpaste or something else that you want, you have to go ask the management to open up the case. We also have high-end companies that looked at this bill and said we may not open up here or expand in New York City because if this bill goes through we're going to be sitting ducks and they're going to be going in and stealing because, I speak to the COs of all my precincts, and they all say the same thing. Nobody's going to jail for property theft. The same person is stealing the cars, the same person, he's arrested, two days out, and he's back on stealing car or stealing catalytic converters or doing other things. I'm also hearing from gas station owners. One gentleman has four gas stations in my District. He says I consider it a good day when I'm not losing 2,000 or 3,000 dollars to theft. Then we have the City Council proposing this, which the worst timing you could imagine, to a city that's still under siege, that's still trying to figure out what are we

doing about property crime, what are we doing to protect businesses that are under siege with shoplifting like your clients, by the way, Jay, they have a small profit margin, don't they?

JAY PELTZ: Tiny. If you're doing 1 percent net nowadays, you're doing well.

COUNCIL MEMBER HOLDEN: That's why we see supermarkets closing. I used to have a lot more in my District, probably triple the amount I have now. People want supermarkets, but if we're not going to allow them the technology to protect themselves, they're going to close so this is what we want because, some of the things I heard today are not even true because the technology, like I said, I've read articles, 95 percent of the time facial recognition is accurate. Is that more accurate than somebody saying I think that looks like the guy, I think this guy is the guy? If they have no technology to verify that, they're going to stop way more people that are innocent. The Police Department uses facial technology almost to a degree where it's actually facial recognition is all, if I had a perp, and I did witness a crime, I had to identify a person, they gave me five pictures, I think it was five, of the

person, it looked like the same person because they have to make it more difficult that you have to be sure that's the person, so it's more difficult. I think you had something to add. I'm sorry.

JAKE PARKER: I was just going to respond and say the problem is this would take away an ability to reduce theft without sending anyone to jail. As the gentleman at the end of the table was mentioning, this was feedback we had from our members that provide services to the retail clients, when you're using systems to simply flag individuals who are involved in this activity, what they are offered is increased customer service in knowing that someone is watching them as they come in the store and there have been instances where stores have seen they've come back less often after a certain number of recognitions. After seven or eight times, they don't show up anymore, and they've been able to reduce theft by 80 or 90 percent.

JAY PELTZ: In our experience, we think that a bill can be done that allows biometric systems to be used for public safety purposes with appropriate safeguards to guard against the (INAUDIBLE)

COUNCIL MEMBER HOLDEN: Yeah. Again, these are amendments that could be done. I'm not saying I'm against this whole thing if we could make it transparent, but we don't take the ability to actually safeguard merchandise because we're going to lose more businesses, and I think it's unconstitutional first of all. That's the bottom line. I'm looking at this, and you can't prohibit a business who invested already, who invested maybe millions into this technology, and we're going to say now you can't use it, which is, to me, I just don't think it's going to, it's going to get challenged.

I just want to say at this point with the current conditions of the City and the current conditions that we're not putting people away and we're talking to everyone, we're talking to businesses that have given up. By the way, the businesses in my District, Chairs, they're telling me they stopped reporting to the local precinct or calling 9-1-1 because they don't come, there's not enough cops to patrol the neighborhoods, and, again, I do listen to the scanner and I do hear that, and if everybody is going to put these legislations together that are going to hurt more businesses than help

them, we have to rethink who we are as a Council so thank you, Chairs.

FRANCISCO MARTE: Robert, we really would love this bill and support if this bill would come with another one that said there's going to start to be consequences for the criminal, for the theft, for the shoplifting. If we have the consequences for the shoplifting, we don't need the camera, but we need to have consequences. When you see people arrested over 30, 40, 50 times, and they come back, you know what it has done to a store owner? They've been arrested, they've caught a shoplifter, they call the police. When they used to come and they're arrested, they come later on, maybe two hours later or the next day, (INAUDIBLE) to the store owners, there's nothing you can do, look, I am now here, you can do nothing to me, so that's what's been happening and that's the sense that is out there. We can do whatever we want because there is no consequence. The police, sometimes they say we don't come because they have to walk out or we just have to give (INAUDIBLE) so, like that, what we need is law and order and consequence so for everyone, when they commit a small crime, they should have at least some type of consequence so they

know that they did something wrong, at least community service day. What happened to (INAUDIBLE) that was with something less than two dollars, three dollars, but it turned to a tragedy. Why? Because there was no consequence. There's no respect. That's what we need. If we have the respect and consequence with the criminal, when they commit a crime, we would not even need cameras, but that's what we need, and that's the support that we need, the Mayor needs to support or the Council Members, we, your constituents, we need your support to bring back the public safety which we already lost. Thank you.

CO-CHAIRPERSON GUTIERREZ: I have one more question and then we can wrap, okay, then Nantasha. What are your thoughts, I understand, you've certainly made the case about how having the option to utilize this technology for your membership and their businesses could aid in preventative theft, and what I would like to know is what is your position on utilizing this biometric information, this data, for other things other than things like theft prevention, like if someone were to petition your members wanting to buy the data for whatever reason? I think our concern is an abuse of this, right, and so right now

there's very little safeguarding, to be honest, with private entities and the way that they're utilizing data and like what they do. Obviously, the MSG and the Dolan example is I think something that is a lot larger, certainly none of your members are doing that because this is MSG and Radio City Music Hall, but I want to ask what is your position on that, like being approached by a data company wanting to purchase the data that your businesses are capturing?

JAY PELTZ: I thought that that was already barred under City Law. That's illegal. You can't sell biometric data, but we're not…

CO-CHAIRPERSON GUTIERREZ: But what we learned today is that there's no real sense if that is actually being enforced is what I'm saying, and we have advocates today that said no, we know it is being sold. I get what you're saying, but for your businesses…

JAY PELTZ: We're only interested in the ability to utilize the identifier information through a system solely for public safety purposes.

CO-CHAIRPERSON GUTIERREZ: For theft prevention?

JAY PELTZ: Correct, and not just theft, but there was an example somebody gave me of how somebody had stolen, there was a relationship that fell apart and the noncustodial parent grabbed the kids and went to a different state, to Jersey, and I forget the facts, but they were able to contact the police in Massachusetts and New Hampshire, and that person was apprehended, the kids were taken away, and then wound up with a relative and then back with the custodial parent, with the mom.

CO-CHAIRPERSON GUTIERREZ: Yeah. Thank you.

JAKE PARKER: I was just going to say, our members, we don't buy or sell biometric data, and I think there's a little bit of confusion about that out there. I know there's concerns about data brokers and what they do. It's a little bit different. Part of that is because of the nature and what biometric data is produced by biometric technologies is. The purpose of biometric technology is to match individuals to confirm so each software platform creates an individual way of measuring your biometric, like your fingerprint, it's not actually a picture of your fingerprint, it's that software's

numerical value it assigns, and so that can only be used inside that software, and so if that were to be stolen or transferred to someone else, they could do absolutely nothing with it and so I think there's just a little bit of misconception there, but, just to confirm, our members do buy and sell data.

CO-CHAIRPERSON GUTIERREZ: Thank you.

CO-CHAIRPERSON WILLIAMS: I lost my notes again. It's too much paper. You mentioned that you would be okay with the bill if there were some changes, you said something to that effect, could you detail what you feel would need to be changed or taken out to be more comfortable with the bill? I'm just interested in your thinking.

JAY PELTZ: We're looking for a public safety exception, and we're happy to engage in discussions to work that out, exactly what the standards would be, with adequate protections to address the legitimate issues that you raised today.

CO-CHAIRPERSON WILLIAMS: Thanks. I had a question for the other guy, but I think, Jake, you can possibly answer it. It's about cyber security. We didn't talk about that so I was interested if his members were looking at cyber security, and I guess

through your company, how are you adjusting and/or prepping yourself, protecting yourself from cyber security breaches.

JAKE PARKER: Biometric data, as I was just describing, it is a form of sensitive personal data that needs to be protected just like you would with other types of data Social Security Numbers, other kinds of identifying data, but the way that biometric data is created and used is actually a natural form of cryptography because without the software or any kind of reference data to compare that against, you can't like, for example, recreate a facial image from your facial template created by the software, you can't recreate an image of your fingerprint from a fingerprint template so that's a natural form of cryptography, but also those templates themselves need to be subject to the best practices for data security and storage such as encrypting, make sure that data is encrypted at rest and in transition, that's very common throughout the industry.

CO-CHAIRPERSON WILLIAMS: Is that you are storing data through like secure encryption systems?

JAKE PARKER: Absolutely.

CO-CHAIRPERSON WILLIAMS: Okay. What about you?

JAY PELTZ: Also to add to that, one of our worst nightmares would be if there was a security breach and people's biometric data was stolen and got out there. The concerns that you've raised are reasonable. We don't like them and we don't want them. This is not what our members want. They're just looking for a targeted exception for public safety purposes.

CO-CHAIRPERSON WILLIAMS: Yeah. I think, I'll speak for myself, I appreciate that, and I appreciate what everyone is saying here, and I think Chair Gutiérrez just also said this is like the abuses of it and how do we protect around the abuses of the technology and then how do we cure once abuses have been made, how are people made whole if there is an abuse or if there is some inaccuracy in a particular technology that might facially recognize somebody that is not actually the person that has stolen from your store 30 times but there's just inaccuracies in a flawed system so how can we, again, cure and make that person whole and then also how do we protect against inherit biases and other things

that might take place for the person who's actually using the technology because I do think that because there is not as much regulation, it doesn't create a lot of space to even try to attempt to provide some type of guardrails around said abuses, and I think that's the intent of a lot of these bills is just to provide some level of guardrails and, for me, even though I might sign onto a bill, when I'm at a hearing, I'm genuinely listening to what everyone is saying even if I come into the hearing with a certain opinion, like I'm genuinely trying to understand what your issues are, how it will impact your business, because I understand we're in a capitalistic society so how is it going to impact your business, how is it going to impact public safety, and ultimately how is it going to impact all New Yorkers and their conveniences. I'm a CLEAR member. I was talking behind him, MSG uses CLEAR so if this bill goes into effect, I technically can't use CLEAR to go into MSG so I'm trying, and I'm just giving you that mindset so you can understand quite frankly my line of questioning because I'm really just genuinely trying to understand what the concerns are, how can we provide some type of guardrails without unintended

consequences that I think a lot of bills tend to have naturally because laws are also not perfect, just like technology isn't perfect, and so for me I'm always trying to figure out how do we mitigate as much as possible some unintended consequences from well-intentioned laws.

JAY PELTZ: Right. I mean that's a fair point. If the goal is to make abusive practices, if abuse is the standard, then you can incorporate that into the bill without being overly broad and banning or over-regulating conduct that's legitimate and that shouldn't be over-regulated.

In terms of people suffering harm, it's the same point. There's a way to draft that clause so that only people who are harmed because of a pattern of bad behavior or willful malfeasance. It's a matter of crafting the right standards so that the bill isn't overly broad.

JAKE PARKER: If I could add to that, I would say that the use of biometric information for commercial purposes definitely should be consent based and, I'm coming back to what we were talking about earlier I think, but there is a model of ways to do that. If you look at the most recent statewide

data privacy measures that have passed in Connecticut, Virginia, some other places and likely to pass in four or five more states this year. They've made sure that personal data is only used based on consent, but they've created a specific exception narrowly defined for security purposes so that's been done already at the state level.

CO-CHAIRPERSON WILLIAMS: Can you say the states again? You said it really fast, and I only got Connecticut.

JAKE PARKER: I'm sorry. Virginia and Connecticut were the most recent states, but a number of others have enacted something similar already this session, Iowa, Indiana will, and several others. Happy to provide more information.

CO-CHAIRPERSON GUTIERREZ: Can I ask one question? How much does it cost a bodega, por ejemplo, to use this technology?

FRANCISCO MARTE: How?

CO-CHAIRPERSON GUTIERREZ: How much does it cost a bodega or a supermarket to have this technology?

FRANCISCO MARTE: It's pretty expensive, 4,000 to 5,000 dollars.

CO-CHAIRPERSON GUTIERREZ: And it's a one-time fee, no?

FRANCISCO MARTE: Huh?

CO-CHAIRPERSON GUTIERREZ: It's not a one-time fee?

FRANCISCO MARTE: Yeah, I mean for one or two cameras, but we only use it in ones that to face the…

CO-CHAIRPERSON GUTIERREZ: The door.

FRANCISCO MARTE: Door, but it's pretty expensive. That's right (INAUDIBLE) we don't have it yet because it costs a lot of money, but little by little we'll be enforcing that because we need (INAUDIBLE)

CO-CHAIRPERSON GUTIERREZ: Okay. Thank you all so much for sticking out.

COMMITTEE COUNSEL BYHOVSKY: Thank you so much for your testimony. Now we hear testimony from witnesses who are here virtually, and our next panelists are Adrian Gropper, Jake Wiener, Elizabeth Daniel Vasquez.

SERGEANT-AT-ARMS: Your time will begin.

COMMITTEE COUNSEL BYHOVSKY: You can start your testimony.

ADRIAN GROPPER: Me?

COMMITTEE COUNSEL BYHOVSKY: Yes.

ADRIAN GROPPER: Okay. I'm Adrian Gropper. I'm the Chief Technology Officer of the Patient Privacy Rights Foundation. As a physician and technology entrepreneur, I'm an expert in the safety and effectiveness of technology in licensed practice. I'm also an invited expert to global standards organizations working on digital identity laws.

I'm testifying to the need to number one, prohibit hidden or unconsented data brokerage of biometrics, and, two, prohibit secret or proprietary technology for biometrics and artificial intelligence.

Biometrics are essentially public, and their risks are vastly increased with AI. Deep fakes are the combination of AI and biometrics. The harm from deep fakes ranges from attacks on the individual to attacks on democracy. Data brokers come in two flavors, open like Facebook or TikTok, and hidden like the thousands that sell commercial surveillance for profit. Either way, there is currently no limit on the ability for data brokerage to leverage AI in developing other more valuable ways to manipulate us.

Regulation of biometrics is tricky because they're essentially public, even DNA can be picked up without our knowledge. Regulation of AI is even harder because the technology is still in its infancy. There are, nonetheless, two obvious ways regulation can mitigate the risks of biometrics and AI, data brokers, and secret privatized technology. Commercial surveillance of biometrics should be illegal. Any service provider that employs biometrics for security or convenience, for example a bank or a notary public, should be absolutely prohibited from interacting with a data broker without consent. The data brokers we call credit bureaus are already regulated, and they should be further constrained from secondary uses outside of strictly consent to credit services. The other point of regulation of biometrics and AI should be a prohibition on secret or proprietary technology. It's hard enough to envision regulating technology for surveillance (INAUDIBLE) but that task is made much, much harder with the technology that's treated as confidential private assets by the operators. Biometric technology and machine learning must be kept open source and in

the public view and treated as public goods, the same way we regulate and label our food. Thank you.

COMMITTEE COUNSEL BYHOVSKY: Thank you for your testimony. Let's move to our next panelist, Jake Wiener.

SERGEANT-AT-ARMS: Your time will begin.

JAKE WIENER: Council Members, my name is Jake Wiener. I am a lawyer at the Electronic Privacy Information Center, also known as EPIC, in Washington, D.C. I study advanced surveillance technologies, including facial recognition, the flaws in these systems, and their impacts on society. As an advocate for privacy and civil liberties, I'm impressed with the City Council's proposed approach, and I urge the Council to pass both bills into law, ensuring that there is a strong private right of action in each bill.

Facial recognition is a dystopian technology, frequently subject to error and bias, and even more dangerous when it works effectively. I'm going to go off script here just to address several points that were raised by industry groups.

First, these bills are targeted. They are addressing places of public accommodation and

housing, and they're very well thought out to address places where consent is not viable.

Second, I just want to say that there is no peer reviewed eviction I'm aware that biometric surveillance systems actually reduce crime, no peer reviewed eviction. At the very best, what these types of surveillance systems can do is push crime around and concentrate it in the poorest communities, providing maybe a little more safety for the rich and increasing harm on the poor and the marginalized. They don't reduce the overall incidents of crime, and I find it deeply ironic that the groups pushing for more biometric surveillance are also the groups citing crime statistics. There is more surveillance in New York City than at any time in our history, and it cannot be that a spike in crime coinciding with the rise in surveillance will be resolved with even more surveillance.

Third, there is no way, and I want to just expand here, there is no way to meaningfully obtain consent for these systems. I want to give you a couple of examples. First, let's talk about an apartment building. Even if you do things like really well, you get consent from every single one of your

residents and they actually want that, you're still not going to be able to obtain meaningful consent from their guests, from service workers, delivery drivers, your plumber, and many of these people who you're giving an illusory choice to. For me, I think about like if I'm invited to a dinner party, I can either go to that dinner party, submit to the scan, not knowing what's happening with my data, not knowing if I'm going to be wrongfully excluded, or I decide to miss out on a social event. For a grocery store, the case is even sharper. You either submit to the scan or you go without food. That is illusory consent; it's not real consent.

I just want to flag I'm happy to answer questions that the Council has on bias in facial recognition systems, why these systems will never stop making mistakes, how NIST testing, although good, falls short, and why biased use is always going to be a risk, but I'm going to focus the rest of my testimony on how these systems harm our society.

I've thought a lot about this, but I want to raise one issue that's not been discussed much which is the potential for facial recognition systems

and other biometric monitoring to create comprehensive…

SERGEANT-AT-ARMS: Your time is expired.

JAKE WIENER: If I can just have like 30 more seconds. Every time you submit to one of these systems, you're creating a record of where you were and when you were there, and as these records compound it becomes essentially impossible for you to preserve privacy in your public movements. This is unique in a certain way to biometric systems because I can leave my phone at home, but I can't leave my face at home. I have no control over my location being logged, potentially being sold to data brokers, given to the police without my consent and without a warrant, and that makes these systems incredibly dangerous, and I welcome any questions. Thank you.

COMMITTEE COUNSEL BYHOVSKY: Thank you, Mr. Wiener, for your testimony. Our next witness is Elizabeth Daniel Vasquez.

SERGEANT-AT-ARMS: Your time will begin.

ELIZABETH DANIEL VASQUEZ: Good evening. My name is Elizabeth Daniel Vasquez, and I'm the Director of the Science and Surveillance Project at Brooklyn Defender Services. I want to thank City

Council and Chairs Gutiérrez and Williams for holding this joint oversight hearing. As we can tell by the conversation that's been had today, this hearing is particularly timely.

As public defenders for the Borough of Brooklyn, we see these systems in daily use, impacting our clients in the criminal legal systems, the family separation systems, and the immigration systems. We've even seen them deployed against our clients seeking unemployment benefits, facing evictions, or calling their loved ones from detention. Underlying the mad spread of biometric identification systems is the national and global expansion of artificial intelligence generally. Computerized pattern matching entities are dominating the news, and their dangers are being debated globally. We've talked about them here today, but to get to the core of the era-defining issue, we need to understand how machine learning or artificial intelligence works. Fundamentally, to build an AI system, we heard this from a witness earlier, a developer needs a large amount of data. Features of surveillance data (INAUDIBLE) faces in surveillance footage form datasets that then get used by big tech.

It's those large datasets that teach AI systems, and, without them, biometric identification systems would be impossible. AI then brings with it a voracious appetite for data, our data. Thus the conversation our community truly needs to have is not one centered around banning individual technologies but instead about defining our rights to our data and particularly grappling with the inequities of the data surveillance economy we are already constructing around ourselves. The single largest user of biometric identification systems in our city is government. Agencies including NYPD, DOC, ACS, the Department of Labor, DHS, ICE, and CBP, and the neighborhoods carrying a disproportionate amount of our city's surveillance load are black and brown. Our city has invested billions in a 20-year surveillance infrastructure building program that relies critically on biometric identification technologies. Despite these investments in deployments, the promised of enhanced public safety has not been realized. Earlier today, the Chief Privacy Officer for the City made the assertion that the NYPD is in compliance with biometric data privacy laws and policies. He suggested that the NYPD has been

transparent about the deployment of these technologies, that the new discovery laws have ensured disclosure if such technology has been used in cases, and that the courts are able to provide oversight to protect our communities' constitutional rights, dignity, and liberty. Each of these assertions is false. As a public defender in this city, we have faced a long history of secrecy on the part of the NYPD, particularly regarding its use of surveillance technology. The OIG's recent report on NYPD's compliance with the POST Act underlies this point neatly. Perhaps, more critically, I can attest as a public defender that the new discovery laws are not being enforced in a way that ensures NYPD disclosure of its use of surveillance technology that relies on biometric information. For example, when the NYPD…

SERGEANT-AT-ARMS: Your time is expired.

ELIZABETH DANIEL VASQUEZ: When the NYPD uses facial recognition cases, they do not disclose, and the DA offices fight disclosing the underlying case files documenting that facial recognition analysis. In many cases, the most we get is a so-called potential match notification report and no

information about how facial recognition tool analysis was actually conducted.

Another example is the Domain Awareness System. The NYPD use DAS in every investigation. In every case, the NYPD does not disclose, and the DA offices fight disclosure of the complete DAS reports that were generated in those investigations. I could continue.

As it relates to the court's ability to oversee the NYPD's use of biometric data, a close examination of the NYPD's POST Act disclosures brings home the devastating reality that I experience every day as a public defender. Despite the comic belief that the courts provide oversight of police tactics, the collection, storage, and use of the vast majority of the NYPD's surveillance data including biometric data will never be reviewed by any court or anyone outside law enforcement. According to its own disclosures, the NYPD does not believe it needs to seek a warrant or court approval to use 3/4 of the surveillance collection methods it has disclosed deploying. In the face of our City's permeating surveillance ecosystem, there is significant urgency for the Council to truly and thoroughly reckon with

the use of biometric identification systems. I would love to talk with each of you more about the threat of the problem we are seeing in Brooklyn and the comprehensive solutions (INAUDIBLE) identify from our unique vantage point in the city. The bills before the Committees today are a step, and they will positively impact the communities of Brooklyn that BDS serves, but they are not enough.

COMMITTEE COUNSEL BYHOVSKY: Thank you so much for your testimony. Our next panelist is Adam Roberts.

SERGEANT-AT-ARMS: Your time will start now.

ADAM ROBERTS: Thank you for holding this hearing today. I am Adam Roberts, Policy Director for the Commissioner Housing Improvement Program, which is also known as CHIP. We represent New York's apartment building workers and owners, and we are here to express concerns about Intro. 1024 of 2023.

Biometric recognition technology is still very new, particularly in its application to residential buildings, and while it may not be widely used now it is likely to become more common across New York's residential buildings in the next few

years. Banning it outright would stop New Yorkers who want to use biometrics in the future from utilizing its benefits. Biometrics may prove particularly useful in maintaining a building's security. Most of our city apartment buildings cannot afford to have a full-time doorman or security guard. Biometrics limit access to tenants, guests, and building workers at a fraction of the cost of full-time doorman. This would also provide significantly greater security for tenants and building workers. Furthermore, biometrics can make building security more convenient for tenants. Though not widespread yet, biometric technology does already exist to allow tenants to enter their apartments without a key. Fingerprints or irises can serve as an additional option for entering (INAUDIBLE) building in the future. In buildings without doormen, this would reduce the burden of forgetting or losing a key. This convenience biometrics provide is already evident, and it is this convenience factor which has made biometrics widely used for entering sporting events, concerts, airports. Considering this, there should be no reason to ban tenants from using biometrics when entering their own homes or workers from entering their

workplace. Biometrics have the ability to be a great equalizer for New York's tenants by providing additional security at a fraction of the cost of traditional methods. They can have very consequential impacts like ensuring access only for tenants, guests, and building workers. Banning biometrics would fall hardest on those tenants who could not afford to live in a doorman building or those workers who are not employed by luxury building owners. We recognize concerns that our privacy and profiling biometrics and, therefore, we hope the Council will redraft this bill or consider new legislation (INAUDIBLE) thoughtfully address those concerns without outright banning biometrics. Thank you.

COMMITTEE COUNSEL BYHOVSKY: Thank you, Mr. Roberts. Our next panelist is Avi Kaner.

AVI KANER: (INAUDIBLE) Hold on. Hello.

COMMITTEE COUNSEL BYHOVSKY: Hello. We can hear you.

AVI KANER: Oh, good, good. Thank you. Hold on, I'll take it off speaker. Hello. Thank you for inviting me today. My name is Avi Kaner. I'm the owner of the Morton Williams Supermarket chain. Our stores are primarily in Manhattan. We have over 1,000

full-time union employees, almost all of them are immigrants. Our stores were open 24/7 during COVID while people were hunkered down in their apartments or fled the city, but now our stores are under assault by theft driven directly and specifically by New York City's refusal to prosecute thieves. Stealing up to 1,000 dollars at a time is now an entitlement in New York City. Just like many drugstores have closed their doors, now many supermarkets are starting to close their doors because they can't handle the crime. You guys are probably too young to remember this, but years ago we used to have Polaroid cameras. We used to take pictures of thieves, scotch tape them by the time clocks, and, if that person were to show up again, we'd confront the person and tell him or her that they can't shop in the supermarket. There's really no difference between that and the facial recognition software. The only difference is the facial recognition software is more accurate, and you're not holding the Polaroid picture and just randomly tagging people because they look like that person. Over the past year alone, our gross margins are down 2 percent due to theft and the City's refusal to

prosecute thieves. Also, last year we spent an additional 1 million dollars in off-duty NYPD officers, we were paying them 45 dollars an hour, now they've raised the price to 55 dollars an hour so we stopped using them, we can't afford to use them. Half of our stores are at risk of shutting down, and that's the last the City, New York City does not want to turn into another San Francisco, believe me, so the City has done enough with its assault on businesses like ours. Many of our employees have been violently attacked when they try to stop thieves, and the police refuse to even arrest the thieves since the prosecutor will not prosecute them. We must have the ability to protect our businesses. We are not collecting biometric data. We're simply using photos of known thieves to prevent their entry into our stores. I implore you to please reject this misguided law, although it's well-intentioned. I agree with you that it's well-intentioned and I would support letting people know that by entering this business they acknowledge that we're using facial recognition to reduce theft and to protect them, but to ban it outright is really a continued assault on business. Thank you.

COMMITTEE COUNSEl BYHOVSKY: Thank you very much for your testimony, and we're moving to our last witness. The last panelist is Hugh Ross.

HUGH ROSS: Thank you. Good afternoon. Hello.

COMMITTEE COUNSEL BYHOVSKY: Good afternoon. You can begin your testimony.

HUGH ROSS: Yes, good afternoon. I'm here as the Chief of Security for the 34th Street Partnership and the Bryant Park Corporation. Bryant Park Corporation and 34th Street partnership are business districts that operate in Midtown Manhattan and are committed to improving these areas by providing security, sanitation services, free public programs as well as events. I have worked for these organizations for 31 years, rising from a uniformed security officer to now the Chief of Security. My responsibility is to provide a safe Midtown environment for the enjoyment of the residents of New York, visitors, and the tourists, and our working commuters. To further this goal, Bryant Park Corporation and 34th Street Partnership has installed and used surveillance camera systems. These systems have enhanced public safety and are an indispensable

public safety tool. Currently, we are working with businesses in the area to obtain (INAUDIBLE) to follow increased safety. Although our BID does not currently utilize facial recognition technology, I believe the technology will also become indispensable to public safety and should not be prohibited. With the increase in mass shootings in public spaces, it will be counterproductive to prohibit the use of this technology. Add to these incidents, the identity of dangerous individuals sometimes before the incident occur. Facial recognition technology could lead to the apprehension of the individuals before a shooting and should save lives. We must also never forget the tragic stories that have struck the City on numerous occasions in the past and I'm sad to say will likely occur again. (INAUDIBLE) facial recognition technology could prevent another 9/11. Facial recognition technology could be used in multiple additional ways to serve and protect New Yorkers. For example, facial recognition can be used to protect victims of domestic violence. Many times, domestic violence perpetrators stalk their victims in the vicinity of their homes or places of work. These systems could provide an early warning signal that

could prevent acts of violence. Moreover, facial recognition technology could be used to locate missing children, adults with special needs such as autism, Down syndrome, and dementia, and victims of kidnapping and abduction. Facial recognition technology is in its infancy and can be a valuable tool for society. I commend the Council for bringing this topic for public discussion but believe the prohibition of facial recognition technology is not…

SERGEANT-AT-ARMS: Your time is expired.

HUGH ROSS: The appropriate course of action and will harm the public and fail to enhance public safety.

I take the opportunity to thank you for the opportunity to address you on this important topic.

COMMITTEE COUNSEL BYHOVSKY: Thank you, Mr. Ross, for your testimony.

I want to thank all panelists today who testified and then turn it to Chair Gutiérrez to officially adjourn the hearing.

CO-CHAIRPERSON GUTIERREZ: Thank you, everybody. [GAVEL]

COMMITTEE COUNSEL BYHOVSKY: The hearing is adjourned.

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 May 15, 2023