CITY COUNCIL
CITY OF NEW YORK

---------- X

TRANSCRIPT OF THE MINUTES

Of the

COMMITTEE ON TECHNOLOGY

---------- X

June 10, 2024
Start: 10:08 a.m.
Recess: 1:53 p.m.

HELD AT: COUNCIL CHAMBERS – CITY HALL

B E F O R E: Jennifer Gutiérrez, Chairperson

COUNCIL MEMBERS:
Erik D. Bottcher
Robert F. Holden
Vickie Paladino
Julie Won

OTHER COUNCIL MEMBERS ATTENDING:
Shahana Hanif
Joann Ariola

A P P E A R A N C E S

Kelly Moan, Chief Information Security Officer at the New York City Office of Technology and Innovation

Chantal Senatus, Deputy Commissioner, Office for Legal Matters at the New York City Office of Technology and Innovation

Nina Loshkajian, Staff Attorney at the Surveillance Technology Oversight Project

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

Shane Ferro, Staff Attorney at the Legal Aid Society in the Digital Forensics Unit

Adam Roberts, Policy Director for the Community Housing Improvement Program

Fernando Brinn, CEO of the Brinn Group

Sharon Brown, self

Jake Parker, Security Industry Association

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

Hally Thornton, Fight for the Future

Daniel Schwarz, New York Civil Liberties Union

SERGEANT-AT-ARMS: This is a microphone check for the Committee on Technology, recorded on June 10, 2024, located in Chambers by Nazly Paytuvi.

SERGEANT-AT-ARMS: Good morning. Welcome to the hearing on the Committee on Technology.

At this time, please silence all electronics. Silence all electronics.

If you wish to testify, fill out a slip in the back of the room. If you wish to testify online, you may do so at testimony@council.nyc.gov. That is testimony@council.nyc.gov.

Please do not approach the dais. At this time, do not approach the dais. If you need any assistance, please contact the Sergeant.

Chair, you may begin.

CHAIRPERSON GUTIÉRREZ: Thank you. Good morning, buenos días. Welcome to our oversight hearing on Cybersecurity of New York City Agencies. I'm Council Member Jennifer Gutiérrez, Chair of the Committee on Technology. Today we'll be discussing New York City's cybersecurity infrastructure, looking at the past as well as into the future.

Cybersecurity is a complex and robust field that requires significant investment and

unwavering commitment. The primary goal of this hearing is to provide a thorough evaluation of our current cybersecurity landscape, emphasizing the journey from past practices to the present improvements under the current Administration, the progress that has been made and to outline our forward-looking strategies in response to the rapidly evolving cyberthreats. Cybersecurity is multifaceted and vital. New York City receives threats of violence, hacking our water supply, disruption of essential services, or compromising the information of hundreds of thousands of vulnerable New Yorkers. We must continuously address and adapt to these challenges, ensuring our systems protect the people, not only from the threats of violence, but also from those that jeopardize their identities and their livelihoods if such information falls into the wrong hands.

Cyberattacks on City infrastructure, leading to data breaches are not just issues of technology. This is also an equity issue. The New Yorkers most likely to become victims of a cybersecurity attack on City agencies are the ones most reliant on our public institutions. If you

receive benefits from HRA, received care from a Health and Hospitals facility, work for New York City, or have children enrolled in our public schools, that sensitive personal data is what's at stake here. To ensure public trust in our systems and operations, accountability and oversight of our cybersecurity protocols is crucial. In 2023, the Chief Information Security Officer of New York City Cyber Command reported that the agency receives up to 90 billion warnings weekly from across all City agencies, resulting in approximately 50 investigations each week. Yet the threats remain. New York City agencies have faced notable cybersecurity incidents stemming from internal system issues, third-party vendor vulnerabilities, or improper conduct by agency employees. Incidents involving the NYPD, the Law Department, NYC Health and Hospitals, the Department of Finance, the Department of Citywide Administrative Services, DCAS, and New York City Public Schools in just the past few years highlight the ongoing risks and the need for sophisticated protective measures. Our City agencies collect vast amounts of data, including personal, biometric, and geolocation information. It's crucial that the Office

of Technology and Innovation, which Commissioner Fraser has emphasized is the central authority for all tech-related matters in New York City, takes full responsibility for both successes and failures within our cybersecurity framework. In this hearing, we expect full accountability and a clear outline of where further investments, staff, and improved processes are necessary. Our focus remains on equity, understanding how all residents are being protected from diverse threats.

To promote responsible data practices, uphold individual privacy rights, and lay the foundation for a more secure, inclusive, and democratic digital future, we also will be considering the following bills in the Technology Committee today, Intro. 217, sponsored by Council Member Shahana Hanif, and Intro. 425, sponsored by Council Member Rivera, both addressing the use of biometric information and, additionally, Intro. 539, sponsored by Council Member Justin Brannan, addressing collection and sharing of geolocation data.

I'd like to thank the Technology Committee Staff, Policy Analyst Charles Kim,

Legislative Counsel Irene Byhovsky, my Chief-of-Staff Anna Bessendorf, and Senior Advisor Anya Lehr for their tremendous work in putting this hearing together.

I'd also like to recognize from the Tech Committee, Council Member Holden, and now I'll turn it to Council Member Hanif for remarks.

COUNCIL MEMBER HANIF: Thank you, Chair Gutiérrez, for holding today's important hearing and for including my bill, Intro. 217, on today's agenda. I am proud that 17 Members of the Council currently sponsor this bill, including co-prime sponsors Chair Gutiérrez, and Council Members Rivera, Williams, Sanchez, Louis, and Marte.

Intro. 217 would prohibit businesses and other places of public accommodation, this includes music venues, theaters, supermarkets, from using facial recognition and other forms of biometric surveillance to verify or identify a customer. This measure is critical to combating wrongful discrimination. Facial recognition tools have consistently been shown to have significantly higher inaccuracy rates for people of color and women. This has resulted in people in these populations being

falsely accused of wrongdoing and denied access to public spaces. It is also a matter of basic privacy. People have a right to access essential places, like grocery stores, without having their personal biometric information, like the shape of their face and the way that they walk collected, used, or sold for targeted advertising or other purposes. Since this bill was heard last session, there have been countless developments that have made the passage of this bill more urgent than ever, including wrongful arrests and data leaks, but the event that stands out the most to me is the Federal Trade Commission's finding in December that the pharmacy chain Rite Aid used facial recognition technology to falsely and disproportionately identify thousands of people of color and women as likely shoplifters, including those right here in New York City. The FTC describes the pattern as follows: Acting on false positive facial recognition matches, employees followed customers around at stores, searched them, ordered them to leave, called the police to confront or remove consumers, and publicly accused them, sometimes in front of friends or family, of shoplifting or other wrongdoing. In one case, a false

match resulted in an 11-year-old being wrongly stopped and searched. I urge those here today to imagine how dehumanizing it would be to be one of these customers. The FTC finding emphasizes that discrimination and harm caused by biometric surveillance is not a paranoid hypothetical or a one-off incident. It is here, it is real, and we need to act. While Rite Aid is now prohibited from using biometric surveillance for the next five years, we shouldn't need a federal investigation and lawsuit to prohibit other businesses from replicating this practice and victimizing more New Yorkers.

I want to stress that the bill takes a measured approach. If passed, customers would still be able to opt in to biometric uses such as pay-by-palm at a grocery store checkout or a biometric travel document verification at the airport. Additionally, businesses that truly need to collect and use biometric technology to carry out core functions, such as custom running shoe store that uses gait analysis, would be permitted to do so. We are pushing for basic consumer protections, not ideological absolutism. Additionally, I want to make it clear that this bill does not impact normal

security tools like video monitoring. I share concerns around retail theft and repeat offenders and encourage the City to support our small businesses with funding for infrastructural security upgrades. However, as evidenced by the Rite Aid case, biometric surveillance is not an effective tool and, in many ways, can make New Yorkers less safe. I reject the premise that facial recognition is an essential security measure. As a Muslim New Yorker who grew up in the post 9/11 era, I'm all too familiar with the negative consequences of using fear to justify excessive and biased surveillance.

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

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

I'll now pass it back to the Chair.

CHAIRPERSON GUTIÉRREZ: Thank you, Council Member.

Before moving on, I'd also like to just read a statement on behalf of Council Member Carlina Rivera regarding her bill, Residential Biometrics.

Good morning, and thank you for holding this hearing, allowing me to deliver brief remarks related to Introduction 425. More landlords are 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 uncommon user misidentification to the potential to increase the presence and accuracy of surveillance. City leadership must establish safeguards that protect rights and increase transparency. My bill before the Committee today would 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 housing advocacy groups have pointed out that this type of technology could further fuel gentrification and displacement of legacy communities. While technological upgrades can certainly provide a benefit, it is our responsibility to ensure that all New Yorkers are protected and taken into account when it comes to the negative effects on our civil rights.

I'd like to acknowledge Council Member Joann Ariola who's joined us for this morning's hearing.

Today, we will hear testimonies from New York City Cyber Command followed by testimonies from the public. Now, I want to welcome Chief Information Security Officer Kelly Moan and Deputy Commissioner, Office for Legal Matters, Chantal Senatus. We've been here before, yes, thank you so much, and I'll pass it back to Irene.

COMMITTEE COUNSEL BYHOVSKY: Good morning, everyone, and before we start with Administration

testimony, I kindly ask you to raise your right hands.

Thank you. Do affirm to tell the truth and respond honestly to Council Member questions?

ADMINISTRATION: (INAUDIBLE)

COMMITTEE COUNSEL BYHOVSKY: Thank you. I heard I do from everyone. Thank you so much.

You may begin your testimony.

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

Since its inception in July 2017, New York City Cyber Command has played a vital role in protecting and defending the City and its residents from the impacts of cyberattacks. Over the last seven years, we have built out security services and increased the cyber maturity at over 100 City

agencies while we work collaboratively with agency partners as well as state, federal, and private entities to safeguard the essential services and data that New Yorkers depend on daily. The City Council, as I am sure you are aware, recognized the significance of our duty when it voted unanimously to add Cyber Command to the New York City Charter in 2020. Our mission, the one that inspires me and my talented team, is to make New York City the most cyber-resilient city in the world. This is no small endeavor. New York City is America's financial, cultural, and media capital, and the size and scale of the City's ecosystem rivals that of most states or federal agencies. New York City is also a target for cyberattacks with a technology landscape that is unparalleled among other cities and states. This requires a unified, comprehensive defense against constant cyberthreats and partnerships from public and private sector as well as the support of the Administration and the Members of this Council.

At the outset of his Administration, Mayor Adams signed Executive Order 3 in January 2022 to consolidate the City's technology Agencies, including New York City Cyber Command, into the newly

created Office of Technology and Innovation, OTI. One month later, Mayor Adams signed Executive Order 10, which further established the roles and responsibilities of Cyber Command, including setting information security policies and standards for the city, directing the City's citywide cyber defense and incident response, deploying defensive, technical, and administrative controls, and providing guidance to City Hall and City Agencies on cyber defense. Executive Order 10 also directed each agency appoint a Cyber Command liaison to interface with us to strengthen collaboration and expand incident response capabilities. As a result, we launched New York City Cyber Academy, a specialized training program to bolster the City's cybersecurity workforce and enhance agency cyber capability. To date, we have graduated public servants from 50 City agencies in three cohorts, with the fourth cohort currently underway. In February 22, the same month that he signed Executive Order 10, Mayor Adams joined with Governor Hochul to launch the first-of-its-kind Joint Security Operations Center in Brooklyn. This 24-by-7, 365 cybersecurity hub situated inside of New York City Cyber Command's Security Operations Center

allows us to coordinate real-time efforts with city, state, and federal entities in ways that bolster the defenses of both New York City and the broader New York State. As part of New York City Cyber Command's role, we provide a number of services to City agencies and assist in implementation of key work streams to bolster agency cyber maturity. These range from technical controls, such as security tools, to administrative controls, such as policies and procedures.

Cyber Command also has consistently worked with City agencies and elected offices to develop cybersecurity roadmaps that prioritize the critical cybersecurity work undertaken by these offices. In October 2023, New York City launched our Vulnerability Disclosure Program, VDP, the first-of-its-kind for our city and the largest for a U.S. municipality, broadening the scope of the City's efforts to identify and address vulnerabilities within its publicly accessible digital resources. The VDP enables IT developers and security researchers to identify vulnerabilities within City-owned websites and systems and responsibly disclose them. It provides rules of engagement and guidelines for

submission and the program complements existing New York City Cyber Command initiatives that facilitate timely remediation of identified risks.

I also want to underscore to the Council that our collaboration extends beyond government partners. Roughly 85 percent of U.S. critical infrastructure is private, so here in New York, we have focused on partnerships in the private sector as well. This means collaborating with banks, hospitals, utilities, among many others, to maintain our collective cyber resilience through cyberthreat intel sharing and joint tabletop exercises. As the City's Chief Information Security Officer, I am honored to serve alongside my dedicated team and our City agencies in furtherance of this critical mission. New York City Cyber Command's expanded organizational structure and alignment within OTI have placed the team in a strong position to monitor and respond to wide-ranging cyber threats.

But as we are all keenly aware, there is no time for victory laps when it comes to cybersecurity. The work is never over. There are no absolutes. There are no assurances that security and operational control measures will be successful in

safeguarding against all cyberattacks. New cyberthreats are discovered daily with increasing sophistication and complexity. In cybersecurity, minutes matter. Having strong partnerships in place prior to an incident across many different sectors are essential, and cybersecurity is a team sport, and New York City Cyber Command is only one part of that team.

Through continuous education to increase awareness of social engineering tactics, our cyber-aware City workforce is also a key line of defense to help prevent cyberattacks. They stand vigilant and trained to report suspicious activity expeditiously. As we look to the future, we will continue to promulgate a holistic approach to strengthen New York City's defenses and adapt to a constantly evolving landscape.

I will now turn briefly to pieces of the legislation for today's hearing. Intro. 425 seeks to amend the Administrative Code of the City of New York in relation to limiting the use of biometric recognition technology in certain residential buildings. To the extent that this legislation

concerns the use of technology on private property, it is not within OTI's purview.

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

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

Intro. 539 seeks to prohibit telecommunications carriers and mobile application developers from sharing a user's location data with another person if the location is within New York City. This bill would also impose monetary penalties for violation of the provision and proposes that the Department of Information Technology and

Telecommunications enforce this measure. Although OTI supports the Council's efforts to address privacy concerns, implementation of this legislation as drafted would not be possible. OTI would welcome discussion related to the intended framework for enforcement under these provisions. Additionally, OTI regulates the rights-of-way for telecommunications infrastructure and does not regulate mobile application developers.

I want to thank Chair Gutiérrez and the Committee Members for your time and the opportunity to testify. I'm happy to take any questions.

CHAIRPERSON GUTIÉRREZ: Thank you so much for your testimony. I'm just going jump right in and you all let me know, oh, I'd also like to recognize Council Member Bottcher who sits on the Technology Committee.

Thank you again for your testimony. I wanted to start with just kind of the lay of the land with the City's cybersecurity program. Commissioner Fraser multiple times has stated that it lives with OTI. Every single agency's cybersecurity safety plan lives with OTI. Does every agency have someone

assigned to cybersecurity or a contact person, just to kind of give us the visual?

CHIEF MOAN: Sure, absolutely. Thank you for that question, Council Member. Every single City agency has security professionals embedded in that agency and also, with the Executive Order 10, has established a Cyber Command Liaison as well and, within those agencies, we work collaboratively with those security teams and IT teams to roll out enhancements to their security program to benefit the community of New York City writ large across 100-plus agencies.

CHAIRPERSON GUTIÉRREZ: Is there a team or a person proportionate to the size of the agency? I'm interested in PD and DOE, these are larger agencies. Is there a cybersecurity team or a person in those instances?

CHIEF MOAN: It's going to span and vary depending on the agency. We have smaller agencies with smaller teams and then we have larger agencies with larger security teams as well.

CHAIRPERSON GUTIÉRREZ: Okay, and those agency teams or individuals, they communicate with OTI regularly, frequent?

CHIEF MOAN: Yes, so we have a cybersecurity engagement program that incorporates cybersecurity road-mapping iteratively with the agency to prioritize critical work streams, and that also is above and beyond just general, being able to talk to the agencies more on a weekly or even a daily basis, depending on what's going on within the City domain.

CHAIRPERSON GUTIÉRREZ: I see, and is there more frequency in conversations with agencies that have experienced some kind of breach or incidents in the past, particularly New York City Public Schools?

CHIEF MOAN: As part of incident response plan and procedures, we also take into consideration any enhancements or additional security controls that can be put in place at agencies upon suffering a security incident, and that is not just routine that takes place, but also something that we look to always prioritize within any agency when we see that there could be improvements to be made.

CHAIRPERSON GUTIÉRREZ: Okay, thank you. I know that Health and Hospitals is not directly a City agency. Do you all have kind of control or a sense of

cybersecurity there in the same way that you do with any other City agency or what are the dynamics there?

CHIEF MOAN: Thank you for that question. I think the reality of the world of cybersecurity within the City's domain is that New Yorkers don't entirely care which agency might be impacted by the incident and they typically feel very deeply when incidents impact them directly, and so our job as the Cyber Command is to work with that broad term of agencies, including Health and Hospitals, to understand what the cybersecurity posture is embedded in that organization and how we can assist to further develop maturity across the cybersecurity journey of all of the agencies, including those that might not properly fit directly within the City's domain.

CHAIRPERSON GUTIÉRREZ: Would NYC Health and Hospitals have their own cybersecurity program and protocol and do they not have to be in communication with OTI?

CHIEF MOAN: They are in routine communication with us. It's a shared responsibility across all agencies, and so we partner with them, not dissimilarly to any of our other agencies. They do have an internal security team, just like other

agencies do as well, and that close partnership continues to promulgate day-to-day on a weekly, monthly basis, depending on the topic.

CHAIRPERSON GUTIÉRREZ: Got it, and what are some other examples of agencies similar to H and H that you all coordinate that are public, private? Is EDC one of them? Do they fall under your portfolio of cybersecurity program?

CHIEF MOAN: We've provided support to agencies like EDC as well and, again, those key work streams that I mentioned in my opening testimony really span from some controls that agencies can put in place due to enhanced configurations, all the way to deployment of tools so it really can span depending on the agency and what type of support and help that they need.

CHAIRPERSON GUTIÉRREZ: Okay. Regarding your particular unit, what's the headcount for your particular?

CHIEF MOAN: We're sitting currently at over 100 employees.

CHAIRPERSON GUTIÉRREZ: Okay, and is that the full capacity?

CHIEF MOAN: We are actively recruiting for vacancies. We have a handful of vacancies.

CHAIRPERSON GUTIÉRREZ: You've had, sorry, say that again.

CHIEF MOAN: We have a handful of vacancies that we're actively recruiting for as well.

CHAIRPERSON GUTIÉRREZ: How many vacancies do you think?

CHIEF MOAN: I can get back to you with the exact number. It's not a very large number, but we're actively recruiting for those vacancies, and then we're also working with OMB to prioritize onboarding of new hires as well that we are in the pipeline.

CHAIRPERSON GUTIÉRREZ: Okay. Do you experience any difficulties recruiting talent?

CHIEF MOAN: Thank you for that question. The cybersecurity workforce globally, I think in the public domain, it's very well-known that there is absolutely a gap in the supply and demand of the cybersecurity professionals just market-wide. I think the last statistic I saw was 4 million professionals there's a gap of between supply and demand. I think in the U.S. it's hitting around 450,000 open

positions that folks are recruiting for within cyber. I think in the City, it's actually quite unique on landscape in terms of recruitment for us. I'm really proud of the mission that we have within the City domain. It's a value add and a value proposition that we can provide to prospective employees. It is uncommon that you are able to directly protect and defend the size and scale of this City. Yes, we are a municipality, but we are on size and scale larger than most federal agencies even combined. My background is actually from the federal sector. I lived in D.C. the majority of my life supporting the federal government, most recently the Department of Homeland Security, and I've got to say that the apparatus that we have here in the City, in addition to the team members that we have on Cyber Command make this an incredibly compelling job and career to have within the City, and we've prioritized not just recruitment, but also prioritizing upskilling, reskilling within this City employee domain. I have a non-traditional cybersecurity background, having not gotten, I guess, a computer science degree for a bachelor's, which is a testament to folks that want to get into this field can, right? Intellectual

curiosity, desire to learn and hard work is what it takes, and so we've launched New York City Cyber Command Academy to particularly promote some of those upskilling and reskilling within City agencies so we continue to kind of solve for the growing supply and demand issue that the industry is facing writ large.

CHAIRPERSON GUTIÉRREZ: Thank you. I know you mentioned that you're obviously still constantly onboarding. How long does that process take from application to hiring?

CHIEF MOAN: Oh gosh, it could really depend depending on the role and the timing of the recruitment cycle. I don't have the exact specifics of the duration of that time. That's certainly something…

CHAIRPERSON GUTIÉRREZ: Is it common that it takes three months, six months?

CHIEF MOAN: We've seen all cases. We work collaboratively and very closely with OMB to socialize positions that we're actively recruiting for that are critical hires so they are aware and are able to expedite that onboarding process for us.

CHAIRPERSON GUTIÉRREZ: Okay, thank you. The financial plan reflects funding for Cyber Command

of 123 million in FY22 and 127 million in each of Fiscal Year 2023 through 2026. As cybersecurity threats continue to evolve, do you anticipate your office will be required to expend significant additional resources to mitigate security risks?

CHIEF MOAN: Thank you for that question, Chair.

CHAIRPERSON GUTIÉRREZ: You can say yes.

CHIEF MOAN: In the cybersecurity realm, we are always looking top of mind to the evolving threat landscape and what tooling or fine-tuning, as we call it, can be put in place to ensure protection and defense of new and novel techniques, right? I expect that to only continue with the growing omnipresence of our interconnected digital ecosystem and, so for those types of conversations, we continue to socialize and collaborate with OMB on any new needs that might be emerging that could come out, again, as technology continues to expand and increase in complexity as well.

CHAIRPERSON GUTIÉRREZ: So you anticipate, generally, probably?

CHIEF MOAN: It will really depend on what capabilities come to market. I can't predict the

market drivers, but we are seeing a continuing expansion of technology vendors and services that like to expand capabilities within its current portfolio, and we always look for opportunities to be more efficient as well and optimize our services with a growing attack surface, essentially a technology ecosystem within the City. It is paramount for us to always reevaluate and fine-tune our ability to expand with those threats as well.

CHAIRPERSON GUTIÉRREZ: Has the agency applied to the Governor's New York State Cybersecurity Grant Plan, which utilizes nearly 6 million from the federal grant program to expand municipal access to state-of-the-art cybersecurity resources?

CHIEF MOAN: If I could ask, what specific grant program?

CHAIRPERSON GUTIÉRREZ: There's a federal grant that was released in August of 2023. The Cybersecurity and Infrastructure Security Agency and FEMA announced the availability of millions of dollars in grant funding for state and local cybersecurity grant programs.

CHIEF MOAN: Taking advantage of grant funding is common for New York City in years past and continuing in upcoming years. We will always take advantage of any opportunity to solicit for grant funds. We currently leverage a number of federal grants to expand our operations.

CHAIRPERSON GUTIÉRREZ: You have applied?

CHIEF MOAN: Yes.

CHAIRPERSON GUTIÉRREZ: Okay, wonderful. I'm going to dig into this deeper, but would love to just kind of start how your office receives and addresses tips from the public. Any kind of cybersecurity or security issues from the public?

CHIEF MOAN: From the public. So it could be a number of different cases. We've actually gotten tips from the public or questions about cybersecurity from the public in a number of different ways, whether that be through downstream at each relevant agency who might be receiving a question, or it could be from elected offices, for example, who've reached out and asked for tips.

CHAIRPERSON GUTIÉRREZ: Is it just an email or what, how does that look like?

CHIEF MOAN: It could be an email or Ask the Commissioner page on nyc.gov, right? It could be a number of different ways. It could also be a tip from an ongoing investigation that might have a nexus to the City domain and City assets as well.

CHAIRPERSON GUTIÉRREZ: Do you know if there is an option if someone were to call 3-1-1 to connect directly with OTI about a tip?

CHIEF MOAN: No, there is not.

CHAIRPERSON GUTIÉRREZ: Okay, and what is the process thereafter after you receive a tip, let's say from asking the Commissioner online, like you mentioned?

CHIEF MOAN: If there's a nexus to City assets or City data, City employee information, right, we'll continue to investigate to determine whether or not it is a valid, either vulnerability or data disclosure, right, so a security incident can come in a number of different forms so we have procedures in place to essentially analyze, investigate, and then provide response and remediation actions should it be necessary.

CHAIRPERSON GUTIÉRREZ: Okay, and do you know what the turnaround time is specifically on like

the agency's website for like drop a message for the Commissioner?

CHIEF MOAN: I can't speak to that directly, but I do want to say the majority of New York City Cyber Command's role is focused on New York City agencies and potential cybersecurity incidents that are impacting City employees and the nature of that through City assets and City data so the large majority and predominantly our role consists of engaging agencies to analyze and investigate cyber incidents should they come up.

CHAIRPERSON GUTIÉRREZ: Okay, so you're saying that in those instances they would know how to communicate more directly with OTI because it's coming from City agencies and staff?

CHIEF MOAN: So what I'm trying to say is the public has a number of different methods to notify should they feel or think that they've encountered a security breach of their personal information, right? Those avenues through the federal government, through law enforcement partners is a different means than New York City Cyber Command. New York City Cyber Command's role is predominantly ensuring the protection and defense of City agencies'

infrastructure and data, including City employees. The majority of our cases that we see are reflecting that rather than public submission. In 2023, as I mentioned, we launched the Vulnerability Disclosure Program, which is a little bit different than what you're describing in that we provide an avenue for security researchers to essentially disclose vulnerabilities that they may have found on publicly facing digital infrastructure, which provides just another intake method for us to analyze, assess if it's in fact a valid weakness or a false positive, which could happen, and then disperse that to the City agency for remediation or mitigation of that risk.

CHAIRPERSON GUTIÉRREZ: Okay, okay, thank you. I have a couple more questions before I pass it to my Colleagues for questions.

My next series of questions are related to data and personal information. We know that often that information is shared between agencies through data sharing agreements. Can you describe the extent to which agencies can share data and how the data is shared from a technical standpoint?

CHIEF MOAN: It will really depend on the use case. I think cybersecurity, our ethos and sort of theme of cybersecurity is to be an enabler, not a blocker and so, from a business perspective, when an agency wants to endeavor to share information, sometimes that is a relatively easy mechanism that's already in place, such as a file transfer sharing site or availability of that capability that already has relevant security protections in place, and sometimes that's an agency that endeavors to take advantage of a new technology or system and wants to deploy something new in their environment, and we have relevant security review processes and procedures to work collaboratively with that agency to vet the solution and assist them in any implementation of security controls that need to be met prior to rollout.

CHAIRPERSON GUTIÉRREZ: And in any of those agreements, do you know if the data is required to be encrypted while it's being transferred?

CHIEF MOAN: We have encryption requirements both in our policies but also in our writers for contractual agreements as well, attachment SEY, which is a security requirement

attachment, and then we also have a cloud services agreement. I think largely as we continue to see the use of cloud, a key theme with cloud is shared responsibility or shared fate model, making sure that we are, as the customer, making sure that the right security protections are in place, but then we're also holding the vendor accountable or the cloud service provider accountable to also make sure that they're meeting the measure of those requirements. We have a really robust third-party risk management program, which includes not just those technical controls, but also procedurally in those contract documentation and writers, which also even denote, again, the reality, which is even if a provider puts all the bells and whistles in place for cybersecurity, the reality is they will likely in their timeframe suffer a cyber incident and, for that reason, it's also important for them to understand and know who to contact us, right, if they suffer a cybersecurity incident, so we can very quickly with the agency assess whether or not there's been any impact to New York City equities at play.

CHAIRPERSON GUTIÉRREZ: In those instances where data or personal information is part of the

data that's being shared with other agencies, is the person made aware or how would I know if I'm a client of H and H that my information is being shared, personal information is being shared?

CHIEF MOAN: While I can't speak to the specifics of notification of the privacy or privacy-related matters related to data sharing, what I can speak to is that data sharing is something that is typically routine depending on the use case and the requirement and need to know, and our City agencies in particular have a keen eye and collaboration with not just their privacy teams, but also their security teams in addition to my office and my counterpart, CPO Fitzpatrick's office, Office of Information Privacy, to ensure that that balance is met, not just from a business perspective, but also from a security and privacy perspective.

CHAIRPERSON GUTIÉRREZ: Do you know if there is data sharing of personal information between City and State agencies?

CHIEF MOAN: I can't speak to that, no.

CHAIRPERSON GUTIÉRREZ: Okay. I wanted to ask, do you know if any and what agencies currently use facial recognition technologies?

CHIEF MOAN: I appreciate the question, Chair. I'll have to get back to you. I, unfortunately, don't have that right in front of me, but I'm happy to get back to you with that.

CHAIRPERSON GUTIÉRREZ: Okay. Is that something that would fall in any of agreements between agency to agency? If an agency is utilizing facial recognition technologies, that's something that OTI should be made aware of?

CHIEF MOAN: We have processes in place for security review of technology, right, so if an agency was looking to leverage a provider that leveraged facial recognition, it may come across our desk because of the nature of the system, right, so potentially it's a cloud system or a system that's connected to cloud infrastructure or they're building something on-premises, depending on what that system makeup would look like, then it might be in front of us for security review and, for that purpose, we would run them through their typical processes and procedures, depending on the nature of the data in use, the classification of the system as well, and we have policies citywide that instantiate that.

CHAIRPERSON GUTIÉRREZ: Are you aware of any plan for the MyCity app in particular to use biometric technology for the utilization of its application?

CHIEF MOAN: Not that I'm aware.

CHAIRPERSON GUTIÉRREZ: Okay. Well, I have some more questions, but I'm going to pass it to my Colleague, Council Member Hanif.

Before that, I'd just like to recognize Committee Member, Council Member Vickie Paladino, who's joined us.

Council Member Hanif.

COUNCIL MEMBER HANIF: Thank you so much. I know you mentioned in your testimony that OTI does not have jurisdiction over Intro. 217. Could you speak a little bit more about why OTI doesn't have overview?

CHIEF MOAN: Thank you for that question. As mentioned in my opening statement, the Administration and OTI continues to be committed with City Council to ensure the appropriate balance between privacy, especially in regard to emerging technology. In terms of Intro. 217, to the extent that the legislation supports biometric identifying

information but it does not apply to government agencies, it wouldn't be within an OTI's purview.

COUNCIL MEMBER HANIF: So OTI's jurisdiction is over government agencies specifically, not what this bill is looking to have protections over?

CHIEF MOAN: OTI supports government operations, yes.

COUNCIL MEMBER HANIF: Understood, okay. You know, this is the second time that this bill is getting heard. This is a re-introduction from last session, and last session as well, the Administration did not send the adequate City agencies to really speak on behalf of Intro. 217, well, what is now Intro. 217, and it is the Council's interest, it's within our interest to want to work with the Administration, as you've mentioned, to have a balanced approach on New Yorkers' privacy, and it's imperative that New Yorkers understand what the Administration's position is on this piece of legislation, though I understand that OTI specifically does not have oversight, but I just want to put on the record that this City Council wants to work with the Administration in the legislative

process for Intro. 217 and the other pieces of legislation, which was mentioned that, again, OTI does not have overview, but this process right now is making it very difficult for us to really advance what would be protections for everyday New Yorkers so I'm just disappointed that, once again, for the second time, the Administration did not send representatives to this hearing who could provide pertinent testimony to this bill and the others on today's agenda.

Chair, I'm going to pass it back to you, and then I'll probably.

CHAIRPERSON GUTIÉRREZ: Okay, thank you, Council Member Hanif.

Council Member Holden has questions.

COUNCIL MEMBER HOLDEN: Yes, thank you, Chair. Yeah, I'm kind of disappointed also that we don't have an opinion on this because a bill that would prevent, or bills that would prevent businesses from using technology that they invested in to protect their business from a number of things, from theft and certainly from people who have caused problems in the past are getting into the business, and even a place like Madison Square Garden, that

obviously somebody could target, and the use of facial recognition is important to protect 15,000, 20,000 people so I think the Administration should have an opinion on this, but the fact that you said you don't on both bills, can you discuss how biometric identification tools are used to improve public safety right now in New York City?

CHIEF MOAN: Well, thank you for the question. First off, I would be happy to take that back and provide a response through my partners within OTI.

COUNCIL MEMBER HOLDEN: Wait a minute, you're in OTI. You have no idea how facial recognition is used to protect us? You're in that business.

CHIEF MOAN: New York City Cyber Command protects and defends against cyberthreats. We have counterparts within OTI divisions that would be relevant in engaging in this matter with you directly, and I'm happy to shepherd that conversation.

COUNCIL MEMBER HOLDEN: Again, I mean, you saw what the bills were. I think somebody could have been here to talk to us about this, what businesses

and residents have the right to do is to protect themselves. If everyone in that building, let's say a co-op, agrees that they should have facial recognition technology to protect their homes, shouldn't they have the right, but we can't get these answers so it's really kind of a waste of time.

Could you talk about facial recognition, how accurate it is? Do you know anything about that, or is that another question that's not appropriate?

DEPUTY COMMISSIONER SENATUS: If I may, Council Members, with respect to what our position is on biometric technology and all emerging technology, we are generally considering the dynamic technology and how it winds up affecting the public with respect to their public information and also public safety. However, given the fact that our authority is over City agencies, we can't opine directly with respect to this. However, if you want to have a more robust conversation about what we would recommend considering as part of…

COUNCIL MEMBER HOLDEN: Wait a minute, first of all, we're not asking… This is something that's under your purview. Facial recognition is part of your arsenal, right? No?

DEPUTY COMMISSIONER SENATUS: The use of biometric recognition technology is something that we review but, in terms of regulating its use for private entities…

COUNCIL MEMBER HOLDEN: I'm not talking about for private. My question didn't mention private. I said, to improve public safety in New York City, how is it used, and you said, we can't talk about that. You guys. Tell me how that's… I just don't understand. How is it used right now by the Police Department, let's say?

DEPUTY COMMISSIONER SENATUS: That would be within the purview of that agency.

COUNCIL MEMBER HOLDEN: That's the Police Department, but OTI doesn't cover that. How is it used in government to get an entry into a government building, a New York City building?

CHIEF MOAN: So, if I may, again, thank you for the consideration in our response. The technology, regardless of its facial rec or another emerging technology that's continued to be discussed in the public domain, there's applicable security review and processes that my office does undertake, regardless of the use case of that technology and so,

to D.C. Senatus' point, having and shepherding those conversations with the business owners or the use case of those agencies that are potentially leveraging that type of technology would be pertinent. I can certainly speak to our security processes and review to ensure the protection of the underlying data at all sensitivity levels, but that is what we are able to discuss today.

COUNCIL MEMBER HOLDEN: Thank you, Chair.

CHAIRPERSON GUTIÉRREZ: Thank you, Council Member.

Council Member Hanif, I think has a followup question.

COUNCIL MEMBER HANIF: Thank you. I totally agree with Council Member Holden. This is quite egregious and very disappointing. I just want to add on. Could you expand on just the position that OTI has on facial recognition as a tool used by City agencies?

CHIEF MOAN: While I can't speak in particular to facial rec, emerging technology writ large, right, the commitment to balancing both privacy and security.

COUNCIL MEMBER HANIF: What are emerging tech?

CHIEF MOAN: Emerging technology could be the use of cloud, it could be facial rec, it could be Internet of Things devices.

COUNCIL MEMBER HANIF: The Administration doesn't have a parameter as to what you all think about facial rec, what you think about cloud, what is there like pros and cons that you're considering as you are all looking into utilizing these mechanisms?

CHIEF MOAN: Just like any new or emerging technology comes into play, there are always considerations from both the business lens and the security lens that we do take into consideration. Obviously, my office is predominantly focused on cybersecurity threats in the evolving landscape and so, as technology continues to be used, even not just for public sector but also private sector, those cyberthreats continue to evolve, my office's responsibility is to ensure we have adequate protections and defense in place.

COUNCIL MEMBER HANIF: Who within the office leads on understanding what the consequences

and what the positive outcomes are of biometric surveillance?

CHIEF MOAN: It would be a collaborative effort with a number of different offices, including agencies.

COUNCIL MEMBER HANIF: Which are?

CHIEF MOAN: A few come to mind, including OTI's participation from a technology perspective, but also agencies that are endeavoring to use that technology as well.

COUNCIL MEMBER HANIF: That's unacceptable. I think, given that we are heading into using more and more emerging technology, whether it be within AI or biometrics, for the Admin to be here and not give us any substance of what you think of each of these or how you all are, even if it's just sharing, these are the specific agencies that are using it, or we work with the NYPD to understand this set of technology or this mechanism of identifying shoplifters or whatever it is. This is really disappointing, given this should be a humongous focus of our City right now and our City's operation. Chantel, did you want to add something to that?

DEPUTY COMMISSIONER SENATUS: Yes, if I may, Council Member. We do have AI guidelines on our website. We do have a unit that deals specifically with creating those guidelines and creating a space.

COUNCIL MEMBER HANIF: So there is one?

DEPUTY COMMISSIONER SENATUS: To develop that technology.

COUNCIL MEMBER HANIF: Does that mean there is one for the biometrics as well?

DEPUTY COMMISSIONER SENATUS: I mean, unfortunately, I'd have to come back to you with more information with respect to that because that is a particular unit.

COUNCIL MEMBER HANIF: Do you know anything about the pilot program that Mayor Adams announced regarding the NYPD collaborating with FUSUS-Axon, which would allow businesses to feed security camera footage directly to the Police Department?

CHIEF MOAN: Thank you for that question. I'll have to get back to you on the particulars of that.

COUNCIL MEMBER HANIF: Okay.

CHAIRPERSON GUTIÉRREZ: Okay, so there's going to be a number of followups, so we'll make sure to get that to you from both Members.

Particularly with Council Member Hanif's bill, Intro. 217. In your opinion, what agency would this fall under? If it's not OTI?

CHIEF MOAN: With regard to the bill, as it relates to not applicable to the use of biometric identifying information within government agencies, right, it wouldn't be within OTI's purview and, as we understand it, it's not applicable to government agencies writ large. We can certainly have a followup and discuss with City Council about that balance that we're trying to drive between privacy and public safety, but I hope that answers your question.

CHAIRPERSON GUTIÉRREZ: Okay, Council Member Hanif.

COUNCIL MEMBER HANIF: Thank you, Council Member Gutiérrez. Given that this is technology that is impacting New Yorkers, when they are experiencing an incident that is discriminatory or biased as a result of this technology, who do they report to? Which is the City agency that would be involved in troubleshooting with this constituent as to the City

having played a part of impacting this constituent or community?

CHIEF MOAN: If I'm understanding correctly, if we're talking about a private sector entity that is leveraging technology that then a New Yorker feels they have been impacted by, there would be a number of different avenues that would be, depending on the use case of impact, and those would largely depend, again, on that use case so it's difficult to give you an answer directly without understanding the details behind it, but we can certainly discuss in further detail the intent of the bill and, again, the commitment that we have to strike that balance that's, oh, so necessary in our world of continuing evolving and emerging technology.

COUNCIL MEMBER HANIF: And what's the balance that you're talking about?

CHIEF MOAN: The balance between privacy and public safety.

COUNCIL MEMBER HANIF: Which is, how are you all understanding that balance?

CHIEF MOAN: That there should be one, given the fact that emerging technology continues to provide considerations for both benefits and

potential considerations that don't benefit the individual that's taking advantage of that emerging technology.

COUNCIL MEMBER HANIF: So in the example of, I'll just provide an example to my previous question. A supermarket is using biometric technology, and I go in and first I get alerted. A red alert comes up saying that I'm a shoplifter, and I refuse that allegation and I want to file a complaint, and so the agency that would administer or support me as a constituent, which agency would be involved in that incident?

CHIEF MOAN: Thank you for that question. At this time I'm unable to give you an agency name, but I am happy to take that back with my partners, not just at OTI, but more broadly in the City agency community and assist in finding a solution to that question.

COUNCIL MEMBER HANIF: Got it, yeah, I think it's imperative for the City to have a response to this and for OTI to know very clearly which City partner would be involved in a case like that one, but there are countless cases and, in my testimony, I described Rite Aid, which we are all familiar with,

and the abuse that is happening by facial recognition technology, when it is totally incumbent on the City to be responsive to both when, let's say this person decides to file a police complaint, is NYPD then investigating and then what does that investigation look like and does OTI have a purview and partnership with NYPD, or for the City to have an analysis of its businesses using this kind of technology that threatens the security and safety of our communities before a crime has happened, right? This is someone who is getting alleged to have done something without there being any substantial proof so those are the two pieces that I'd like some answers, some tangible answers from the Administration because I do think this is an issue that concerns our City and the Administration should have a response and a position on biometric technology. Thank you.

CHAIRPERSON GUTIÉRREZ: Thank you, Council Member Hanif.

I believe Council Member Paladino has questions.

COUNCIL MEMBER PALADINO: Good morning and thank you for coming.

About 20 years ago, I probably would have said no to any kind of cyber anything, recognition, facial recognition, anything because it's an invasion of one's privacy to a point. However, living in the days that we're living in right now, I believe it's absolutely and should be required for, as my Colleague brought up, there's several different layers of it. If you live in a co-op and just simply ringing the bell and buzzing somebody in or they talk to you and you're still not quite sure who it is and that co-op board decides that they want to use facial recognition, then they should be allowed to use facial recognition. I believe facial recognition should be in every government building that we have today if that's required. I believe our police force should be allowed to use facial recognition for the simple reason being it's a more accurate way of asking somebody for just a description of someone. It led to a lot of wrong arrests and undue prosecution. I mean, there was prosecution that was done to people that were innocent. Facial recognition is 100 percent or 99 percent accurate. I'm curious though, I do have a concern. When we go to the bill that's being introduced by, it's 539, as a parent, they're using

technology to track their kids, that's a must. Are there warnings on the apps that will let the people know that their location data can possibly be shared with a third party? That I have a problem with. Also, what is an example of a third party that data would be shared with and, just to be clear, I don't agree with any of it. I find it kind of creepy. I want to know what my child is doing, but I don't want anybody else to know what my child is doing or where my child is. That's my business. There's also a financial question. Who is going to be responsible for the financial burden put on businesses and landlords that have already invested in biometric identification data technology as they would be asked to remove or to replace or to adjust their current BID technologies. Privately owned anything should be allowed to do whatever they want. If they want to have facial recognition, they should be allowed to have it. I voiced my opinion already, and it's a must have tool for our Police Department and, anybody who's got a problem with that, that's really too bad. Thank you.

CHAIRPERSON GUTIÉRREZ: Okay. Thank you. Do you want to respond to any of that?

COUNCIL MEMBER PALADINO: Well, I asked about financial. You want to go to that? Who's going to be responsible for the financial burden put upon businesses and landlords? Who are the third parties in sharing data? That's question two. And I know there was a third. Okay, we'll start with those two.

CHIEF MOAN: While I can't speak to the financial burden that you referenced, as far as Intro. 539 in particular, OTI and the Administration would welcome any ongoing conversations related to the proposed implementation framework as it relates to this particular bill, in particular, having a greater understanding of what that framework, the intent of the Council's proposal would be in terms of a framework. As I mentioned, OTI does regulate the right-of-way for telecommunications infrastructure through our franchise group but does not regulate mobile application developers so that would be a conversation we would love to have.

COUNCIL MEMBER PALADINO: Okay. Concerns for cyberattacks on our infrastructure by terrorists. Is our country equipped to handle an infrastructure cyberattack? I don't think so.

CHAIRPERSON GUTIÉRREZ: You can respond to whether or not the City in our capacity, OTI is equipped to respond.

CHIEF MOAN: Thank you for the question and, again, I want to reiterate, thank you for having me here. These types of conversations are absolutely important and critical to, again, elevate the conversation about cybersecurity within the public domain and public awareness. New York City ecosystem is vast and complex. We have to protect everything from the most basic technology, think your Windows device at home, your Windows workstation, all the way to the more advanced, such as industrial control systems. That mission is incredibly important to us. We endeavor to make New York City the most resilient city in the world, and we do that in a number of tangible ways. I do think it's important in this particular space, what I can disclose, again, in the public domain and in our world, the cybersecurity industry writ large, we're continuing to see trends of threat actors that attempt to trick users through social engineering tactics to click on malicious links or documents. We have to contend with a number of threat actors, three that come to mind in terms of

threat groups or hackers or threat actors that endeavor to promulgate some of these attacks within broadly, globally. One, we have to contend with attackers like hacktivists who are promoted and are fueled by activists and activist causes. We have to contend with cybercriminal groups, which continue as an industry, continues to be omnipresent within the domain. These are threat groups that actively are attempting to gain financially through cyberattacks. And then the third, which again, I think it is important to discuss openly, and again, this is public information, but threat groups such as advanced persistent threats, and those are highly sophisticated threat actors, incredibly well-versed in cyberattacks and intrusion methodologies. In particular, our City continues to be hyper-focused on all threat groups that attack any public or private sector entity but, in particular, there is continued cybersecurity advisories from the federal sector and international partners that have been released related to a threat group known as Volt Typhoon, and the reason I bring that particular threat group up is because we're continuing to see targets against critical infrastructure being omnipresent in the

industry. This particular group, as one type of advanced persistent threat, uses tactics that we call living off the land. It's essentially where a threat actor attempts to hide in plain sight of devices using tools on your computer that your system administrators would normally use, right, known good applications essentially behaving badly, and so this particular threat actor and these living off the land techniques, camouflage techniques that threat actor use are obviously more sophisticated types of techniques, but it's still those that we have to contend with, and as the rise of critical threats against critical infrastructure, in particular utilities, waste and water systems, it is paramount that we have partnerships and collaboration in place to protect against those attacks and defend and then recover from them as well to make sure that we're focusing not just on defense and protection, but also on our incident response capabilities, which includes tabletop exercises with private and public sector partners to, again, continue to practice incident response techniques and protocols should we suffer an attack at any size or scope of any magnitude. Those are just a couple examples of what public and private

sector entities have to contend with from a threat attack perspective. I'm incredibly proud of the team that we had and the abilities that we've been able to build over the last seven years with regard to security services and the partnership quite frankly.

CHAIRPERSON GUTIÉRREZ: I'm just going to ask a couple more questions and then pass it to Council Member Ariola.

I'm glad you finished on the partnership piece. What can you tell us about OTI's current stage of partnerships with small businesses or other companies that operate to digitally protect infrastructure?

CHIEF MOAN: Thank you for the question. Partnerships really span on the cyber realm, size and scope from private sector entities of critical infrastructure providers, like I mentioned, utilities, hospitals, wastewater treatment facilities, all the way to security researchers with our VDP program and, at a high level, it is important for us to maintain general awareness of their cybersecurity posture, but also who they are, right, a human behind the company, right, so that should

they suffer a cyber incident, they also know who we are.

CHAIRPERSON GUTIÉRREZ: Are there current relationships or partnerships that you all have now with some of these entities?

CHIEF MOAN: Yes, yes.

CHAIRPERSON GUTIÉRREZ: Okay, can you name some of them?

CHIEF MOAN: In this particular public domain, I'm happy to offer that up in private, but it ranges really every sector and, again, that speaks to the whole-of-society and whole-of-government approach to cybersecurity because we are all facing the same types of threats and threat groups, and we all are endeavoring to protect and defend and so, when we see something, we say something to our partners, right? If we see an ongoing campaign that could be targeting a partner, we share that information and give them real insight to the extent we can and we have that insight so they're able to better protect them.

CHAIRPERSON GUTIÉRREZ: So there is an existing footprint of a partnership with businesses with regards to both Council Member Hanif's bill and even Council Member Rivera's bill, which is related

to tenants, primarily in private buildings, is there a pathway there for these partnerships to achieve the same mission, which is to protect New Yorkers? If you have existing relationships with, or partnerships with small businesses now, is there not potential to do that with a Rite Aid, for example, or some of these businesses where New Yorkers are explicitly saying that their rights are being violated based on biometric data collection?

CHIEF MOAN: In terms of partnerships, our focus is cyberthreat intelligence sharing and making sure that we're protecting against cyberattacks. I think within the confines of that, that absolutely makes sense within the confines of the cybersecurity realm. As it relates to these particular bills, that would definitely be something that I think a discussion would be needed to understand the intent of that particular framework.

CHAIRPERSON GUTIÉRREZ: Okay. Thank you for clarifying that. The New York City Cyber Critical Services and Infrastructure Project, or CCSI, was announced in 2019 as a partnership between the Manhattan DA's office, PD, and Cyber Command along with a non-profit, Global Cyber Alliance, as a way to

coordinate cybersecurity efforts and responses between the public and private sector. Can you share a little bit about how this partnership has worked thus far, and how OTI works as a part of this initiative?

CHIEF MOAN: Absolutely, thank you for the question. CCSI really speaks to how much thought leadership has been in the City for so long on matters like protecting critical infrastructure against cyberattacks. The threats against municipalities, state, local entities, even federal sector continues to be on the rise even since 2017, since the inception of Cyber Command. The announcement of the Joint Security Operations Center is really just a doubling down of an expansion of the CCSI initiative, bringing together all of those partnerships that I mentioned earlier. In addition to expanding our footprint of those partnerships to ensure that we have the collective good in mind as it relates to sharing cyberthreat intelligence information, and we've even gone so far, especially over the last couple of years, to continue to focus heavily on joint public-private sector tabletop

exercises as well, making sure that we have a keen eye towards that.

CHAIRPERSON GUTIÉRREZ: Okay. I just want to touch on one more question before passing it over to Council Member Ariola.

You mentioned in your testimony the City's first Vulnerability Disclosure Program. I know it's fresh, but can you share a little bit more on this, kind of like on the idea, and has it worked, have you had folks already disclose, and you have to educate me, is this like an annual disclosure or is this just as soon as there's an issue, staff is able to disclose?

CHIEF MOAN: Thank you for that question. We were really proud to launch the VDP program. Obviously, New York City is very large, so endeavoring to launch a VDP of this size was a Herculean effort and making sure that we had the appropriate processes and procedures in place. What's really exciting from a practitioner perspective is that security researchers are out there in the community testing independently the software you use at home. It's part of the reason you get the software updates with security updates embedded in them on

your home computer, right, and so when they identify that there could be a vulnerability that is located within the City domain infrastructure, more specifically, public-facing infrastructures or public-facing websites that New Yorkers interact with on a daily basis, they are able to submit the technical details of that exploitation that they believe is valid to our team, and we are able to assess whether or not it is, in fact, valid, and it's, in fact, an exploitable vulnerability or weakness in the system, and we follow best-in-class industry practice for categorization of severity of vulnerability, and then we work closely with the agency to either put a remediation in place or a mitigation through technical controls and then, once fixed, we also are able to give a head nod to that security researcher on our public-facing portal that says they were able to find something. While we don't reveal, obviously, the specific content of the exploitation for obvious reasons, we don't want threat actors to actually have insight into those vulnerabilities in particular, they are able to get an accolade on the website that says they were able to fix things, and we've done quite a bit to promote

the program, but it is still early on in its tenure so our security researchers have identified a handful of vulnerabilities that have been able to be mitigated, which is a big success for us. Again, a partnership with the industry writ large is paramount because we are so big. It takes all of us as a team to be working together to protect and defend, and I anticipate that will continue to exponentially grow as the program with engagement such as this continues to be in the public domain.

CHAIRPERSON GUTIÉRREZ: Can you share how security researchers are able to submit vulnerabilities?

CHIEF MOAN: Yeah. As soon as a researcher identifies what they believe is a vulnerability that could be exploited, they're able to submit through our online portal and, again, this is public-facing portal, the details of that submission and engage directly with the team to analyze whether or not it is valid. For example, it's very routine for, there might be some back and forth between the team through the intake method to ask some followup questions to make sure that we are able to correctly identify the

means or the tactics being used to exploit to then prove out if it's a valid vulnerability.

CHAIRPERSON GUTIÉRREZ: Is the online portal also an app, or are they only able to access it from their work computers?

CHIEF MOAN: It's just an online portal, no.

CHAIRPERSON GUTIÉRREZ: Okay, and so the NYC Secure mobile app, is that still alive?

CHIEF MOAN: NYC Secure is absolutely our mobile app. For those of you who might not be aware, we offer a free mobile app for New Yorkers to protect themselves against mobile threats. It's called NYC Secure, and it's still available. You can download it for free on the App Store or on the Android Store, and it's just one of the methods to, again, assist the average New Yorker from ongoing threats potentially perpetrated on their mobile device.

CHAIRPERSON GUTIÉRREZ: Your eyes kind of opened up a bit when I mentioned it. Do you know if this app is updated frequently?

CHIEF MOAN: Yes, absolutely.

CHAIRPERSON GUTIÉRREZ: Okay, I'm going to check it out right now.

CHIEF MOAN: Yeah.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF MOAN: Yep, it's on my phone as well.

CHAIRPERSON GUTIÉRREZ: Great, all right, I'm going to pass it to Council Member Ariola and then Council Member Bottcher if he comes back for questions.

COUNCIL MEMBER ARIOLA: Thank you, Chair. I want to go back to the cybersecurity protocols. You talked about several protocols and measures that are in place. Are they publicly available, or would that be not available publicly because of security reasons?

CHIEF MOAN: Typically, specific incident response plans and procedures aren't made publicly available. We also don't want to promote threat actors having an understanding of what we would do should an incident arise to a certain severity level, but those are internally circulated, and agency teams also maintain specific incident response procedures for downstream with their agency in close collaboration with us as well.

COUNCIL MEMBER ARIOLA: Okay, and how often are they reviewed and updated, where you have an internal conversation about what's working, what isn't, so how many times is that done?

CHIEF MOAN: We have citywide policy for incident response plans, and we update, and also in that policy, I believe it's no fewer than annually it needs to be updated but, in reality, updates would come in the form of post-tabletop exercise, testing the plan, realizing we need to tweak this playbook line item versus a procedure because the nature of agency engagement has changed or we've updated considerably since the realignment with OTI has taken place as well.

COUNCIL MEMBER ARIOLA: Okay, and according to the Citywide Cybersecurity Inventory Policy, which is applicable to all systems that connect to a City-owned network, Cyber Command must audit covered organizations for compliance and notify the First Deputy Mayor if it finds noncompliance. The policy further states that Command may conduct periodic audits to review a system's cybersecurity and related information. How many times have you carried out this audit, and how many times did you

report noncompliance in the last two years, if you have that information?

CHIEF MOAN: While I can't go into particular specifics, given the public nature of this hearing, I am also happy to offer a followup in particular for that question. We routinely engage any method, really, including audits and assessments, to understand evolving cyber landscape and posture of our City agencies, including their journey in maturation, right? As I mentioned before, our agencies span from smaller to larger agencies and also in complexity, and so making sure that we're partnering with them to engage and promote cyber maturity and enhancements at the agency is paramount, which is why we have a cyber road-mapping process that actually takes into account any findings or weaknesses that we've identified or third parties have identified that can be improved, and we implement those into our collaborative roadmaps that we work with agencies to develop so then they implement those remediations or mitigations as a prioritized work stream.

COUNCIL MEMBER ARIOLA: Okay, and just, if you could, anything that you cannot share here today

publicly, you share with our Chair in private so she can share with the rest of the Committee. Thank you. Thank you, Chair.

CHAIRPERSON GUTIÉRREZ: Thank you, Council Member Ariola.

I will ask some questions until Council Member Bottcher gets back.

Can I just ask one more question regarding operations? I know the City has a variety of legacy systems powering agency operations. Does OTI have any mechanisms to track those legacy systems?

CHIEF MOAN: As technology modernizes, including specific software or hardware that becomes end of life, per se, that is something that we typically have visibility on and are able to track remediation of. The modernization journey of a city this large, but more broadly of any private sector entity as well, those updates or modernization efforts are routine and continual and, as we look to the future, we continue to promote secure and secure-enabling technologies that really meet the mission of what each agency is endeavoring to do and promoting services to New Yorkers.

CHAIRPERSON GUTIÉRREZ: Great. Thank you. Do you have staff that conduct exercises to practice cyberattack response and recovery?

CHIEF MOAN: We do.

CHAIRPERSON GUTIÉRREZ: You do? Okay. I won't ask anymore. I feel like that's enough.

I wanted to ask about just citywide policies and protocols. In 2020, Local Law 89 passed that requires New York City Cyber Command to ensure compliance with policies established with Cyber Command. How do you all ensure that agencies comply with those policies and protocols?

CHIEF MOAN: Thank you for that question. As part of any cybersecurity program, both compliance and non-compliance are taken into consideration as folks continue to promote and use new and emerging technology. We have escalation procedures in place and timeframes for remediation that are leveraged to ensure that there is a balance of both security and business operations. We do have an understanding that no system is 100 percent secure because we have users, right? We need to be able to operate on a device, and so making sure that we're escalating, leveraging those procedures, should we see a non-

compliance matter or should we see, for example, we've last year alone, we saw, we continue to see in the industry a large omnipresence of zero-day vulnerabilities and, for the public that might be listening, a zero-day is a vulnerability that's disclosed without a fix, without a security update available, and so we have procedures in place with timeframes for remediation for a reason. We want to build the muscle and the dexterity of agencies to be able to fix things fast so that if we see an emerging or an emergency vulnerability like a zero-day come out, we're able to affect that change even faster because we have appropriate processes in place and the agency has that muscle to then go out and do the things that we're asking them to do.

CHAIRPERSON GUTIÉRREZ: In the instance of a zero-day scenario, which as I understand, it's a little bit more specific than like a full-on or different than like a full-on data breach, how do you all adjust the policy or protocol with that agency after that kind of an incident?

CHIEF MOAN: Let's first talk about the zero-day vulnerabilities. If a critical vulnerability, that severity level comes out with a

zero-day, we very rapidly engage our City agency teams to determine what our potential exposure could be as part of our Unified Vulnerability Management Program and, again, I'm speaking at a high level, but I want to provide as much detail as I can because this is an important core tenant of any cybersecurity program and this is where it all starts, right, so when a zero-day vulnerability is disclosed, we very rapidly engage. We also determine what fix could be in place and large in part, most zero-days, the nature of the definition, they don't have a fix, so sometimes we have to put in a compensating control, which is essentially a mitigation of the risk or we have heightened monitoring to determine if we've been impacted in any way, and that's close collaboration with our agency partners, and then in the unfortunate event that a zero-day vulnerability has ultimately led to a security incident, which has ultimately potentially led to a data breach, which is a breach of information that could come from a security technical incident, then when we work together collaboratively with our partners, with our agencies to determine what, if any, data elements were impacted and then send out relevant notification as

it relates to whichever regulated data has been impacted in that regard.

CHAIRPERSON GUTIÉRREZ: I guess as much as you can share about the regularity of updating the policies, like I understand from your previous response, it really just depends, but what can OTI say to the public about ensuring that the policies are being updated, that they're relevant, that they're audited, I don't know if you all do that as well, but what can you all share with us about those particular protocols?

CHIEF MOAN: Absolutely, thank you for the question and for the opportunity to share. We follow best in class industry best practices for remediation timelines for, let's say, vulnerabilities and our associated Vulnerability Management Program. We've also at times actually followed the federal government with regard to advisories such as directives for emergency and critical so these are important and urgent ongoing exploitation of vulnerabilities from threat actors, and so we have our routine timelines in place and associated policies that are updated when they need to be updated if the threat landscape changes, but we also

have heightened directives that we've pushed out in particular when we see that there's an ongoing threat of exploitation and we're seeing that the federal government or our counterparts at the cybersecurity and infrastructure security agency putting out a directive that impacts federal civilian agencies. We typically mimic that and actually push out one of our own for our City agencies as well because, again, it's industry best practice and we want to make sure we're doing everything we can in furtherance of protection of New Yorkers data.

CHAIRPERSON GUTIÉRREZ: Thank you. I'll just have one more question before passing it off to Council Member Bottcher.

According to Citywide Application Security Policy, NYC Cyber Command can conduct periodic audits to review the security posture of any information system. Can you share how often your office engages in this application audit?

CHIEF MOAN: The City has a number of applications, a large number of applications. We routinely engage our agency partners for periodic reviews of those particular systems. And I think it's important to note this, right, so we also engage for

assessments or heightened reviews of systems should we see that there could be an ongoing threat that could potentially impact that system, right? We have a whole of defense, a defense-in-depth approach is what we call it in the cybersecurity world to all systems that are built within the City, and that's not just us, that's also our agency partners, but I'll give you an example. Over the last few years, again, given the geopolitical drivers and what has been happening in the world with multiple protracted conflicts in multiple areas of the world, the threat landscape has continued to evolve. Tactics that really have been used historically like denial of service, where it's a threat actor's attempt to shut off access to a system that is used by, in this case, the public. We're seeing and we saw for the last few years that that changing threat as a tactic that was being used more, right, and so when we saw that it was being used more, we wanted to rapidly engage and continue to engage our agency partners to say, okay, do we have the appropriate protections in place, and so that is an everyday conversation with us and our agencies and, again, that's just one example of numerous examples about how the threats continue to

shift and shape in our job, and what we consistently show up to do with a very immense passion to do so is working with our agencies to understand the why behind why we're asking them what they need to do, them understanding it, and then ultimately, I'm a New Yorker, my team are New Yorkers, we're protecting not just our data, we're protecting our families' data, our friends' data and so making, I think, that sense of passion and commitment to service to the City of New York is really what I believe best position us to protect and defend against these threats.

CHAIRPERSON GUTIÉRREZ: Thank you. I'll pass it to Council Member Bottcher for questions.

COUNCIL MEMBER BOTTCHER: Hi. I'd love to hear your personal perspectives on the issue of facial recognition technology as someone who's worked in the cybersecurity space for many years, as someone who worked for federal security agencies. What are your views about facial recognition technology, both in the private sphere and the public sphere, and what is the balance, in your view, between the benefits of new technologies and the potential threats to civil liberties?

CHIEF MOAN: Thank you for the question again. I think, while I can't speak specifically to facial recognition, what I can speak to is technology writ large. We're continuing to see emerging technology promulgate through the industry. This isn't something new or novel to the cybersecurity realm. For example, artificial intelligence, as it relates to cybersecurity, is a topic that was in consideration many moons ago, many years ago. In addition to our interconnected city, the use of Internet of Things devices, IoT devices, so think your smart fridges, your sensors that are being deployed, those all have access to the internet, and that presents unique challenges from a protection and defense perspective for cybersecurity because large and part folks that may not realize they're leveraging that technology and could be exposed from a cybersecurity perspective so I think the federal government has done a really great job, in my opinion, in particular the Cybersecurity and Infrastructure Security Agency, of promoting awareness campaigns such as Secure Our World to promote effective techniques to protect and defend against cybersecurity attacks, the use of

passphrases, right, so remember your password better. Just think the longer the password, the better, four or five words strung together, a special character in between, maybe an uppercase letter, lowercase letter. Studies have shown that that provides more protection than not, than even your most complex password. The use of multi-factor authentication and also just making sure your devices are updated. Those are three core principles that every New Yorker should take into consideration in their personal life, but we've also heard and continue to see, and we promote in the City, secure by design and secure by default concepts, right? We know that no technology is 100 percent guaranteed to not suffer from a cyber incident, nor is any organization, but we have seen that there should be greater emphasis, and the federal government has taken the pen to this, and even the National Cybersecurity Strategy identifying that there is a risk to contend with with interconnected devices, in particular IoT, and the use of secure by design and secure by default helps protect and defend against those risks.

COUNCIL MEMBER BOTTCHER: Have you worked with facial recognition technology in your

professional background, both in Washington and New York? Has this issue come up much in your professional career?

CHIEF MOAN: Well, like most things, I think the City of New York continues to be a leader in a number of different spaces. I say that in the cybersecurity realm given our size, scope, and autonomy to impact change, but I would also say that in this particular regard, it continues to be a leader in the municipal space, and conversations like this are important ones to have, and I think that commitment to balancing privacy and public safety is one that needs to be contended with and discussed.

COUNCIL MEMBER BOTTCHER: Writ large, what's your view about legislating on this technology? Do you think that government should be playing an active role in legislating in the space of facial recognition, or do you think there should be more of a hands-off approach?

CHIEF MOAN: Well, I can't speak to specifics on behalf of the Administration. I think that the commitment is absolutely there to work with you all to balance that approach.

CHAIRPERSON GUTIÉRREZ: Thank you, Council Member Bottcher.

I'd like to get into just a couple of questions about vendors. Just based on previous hearings or previous remarks, can you share what role Cyber Command plays in negotiating tech contracts for the City?

CHIEF MOAN: We don't play a direct role in terms of negotiation of tech contracts, but we certainly support ongoing conversations with any agency that is looking for advice or has questions about entering into a relationship with a vendor, in particular, that's from the security requirements perspective, right? We have security requirements and citywide policies and procedures related to those requirements for vendors, depending on what the vendor is providing to that particular agency.

CHAIRPERSON GUTIÉRREZ: And I'm sorry to interrupt. Does the agency have to seek OTI, if they're seeking specific support, are they seeking OTI for their review or is this just in every single tech contract, OTI is there to support?

CHIEF MOAN: So it could come in a number of different forms, right? So a large majority of the

cases are through new systems or applications that are being built within the City domain and, if those are leveraging the cloud, for example, OTI has a cloud review process. Security is just one component of that, but not everything is built in the cloud, and so we have obviously even application security, but more broadly security requirements documents made available for every agency, and we certainly offer up conversations and questions and answers should agencies have questions.

CHAIRPERSON GUTIÉRREZ: Is OTI looking at every single tech contract from agencies?

CHIEF MOAN: From a technology contractual perspective, OTI certainly has a large predominance of engagement with agencies more broadly, and that can come in a number of different forms, right, so it could come from the cybersecurity lens, but it also could come from like counterparts at the relevant divisions, whether that be research and collaboration, right, with the AI action plan that the team has in close collaboration with my office has built all the way to infrastructure management who actually supports and builds the systems that most agencies actually leverage or host agencies all

the way to the information privacy office as well so it really can span. I like to think that we're all one big team that are supporting our agencies and whatever questions that they have, if they're security, they come to me, if they're otherwise they go elsewhere.

CHAIRPERSON GUTIÉRREZ: Thank you. I'm glad you brought up the cloud review process. Can you share a little bit more about the role that OTI plays in that procurement process for cloud-based services?

CHIEF MOAN: Yeah, so OTI cloud review takes place within the broader community of OTI divisions. As I mentioned, security is just one of those, and so OTI has launched in 2022, actually launched a strategic plan and has a technology strategy related to the digital ecosystem of the City, and so cloud review is one component of assistance that provides insight into agencies who are building systems that maybe don't realize that they can take advantage of OTI in-house solutions or an opportunity to offer economies of scale, for example, to make sure that the City is getting the best capability out of a vendor community or it's a new and novel technology that requires enhanced

security review regardless of it being built on cloud, maybe it's on-premises and then they work with my office to do so as well.

CHAIRPERSON GUTIÉRREZ: Thank you. Would you be able to share what agencies are or have sought or are utilizing cloud-based services? Excuse me.

CHIEF MOAN: Say that last part again. Are you able to, I tripped over my words, I'm sorry. Are you able to share which agencies do utilize cloud-based services?

CHIEF MOAN: Not off the top of my head, but it's absolutely, the use of cloud continues to be, I like to say that the City is cloud smart, not cloud first, right, so a lot of things make sense to go into the cloud that aligns to our technology strategy and, again, making sure that we're securely developing the cloud is also paramount. Most agencies do leverage cloud services, and so our tech ecosystem is quite vast and where there's opportunities to enhance or optimize those services, especially from a security perspective, we take full advantage of that.

CHAIRPERSON GUTIÉRREZ: Thank you. Does the City have an insurance policy against cyberattacks?

CHIEF MOAN: The city maintains self-insurance.

CHAIRPERSON GUTIÉRREZ: Okay, so no.

CHIEF MOAN: It's self-insured.

CHAIRPERSON GUTIÉRREZ: Okay, that's a no. Okay. In the event of a cybersecurity incident resulting in a data breach, who is responsible? The City or the vendor?

CHIEF MOAN: It depends. I think that's a great question to unpack for a minute. We've seen, and again, the sector writ large, this is all public information, has seen a number of different types of attacks. One could be an incident that has impacted an agency directly, not through a third-party compromise like a cloud service provider, right, and so relevant victim notification through our citywide contract would, if the data impacted was regulated data, right, those particular data elements, then victim notification would be in effect and take effect. Part of our third-party risk management strategy is not just, as I mentioned, the technical controls or the administrative controls, but also making sure we have a mechanism to understand and have a relevant victim notification in place should a

third party be victim to a cybersecurity incident that then impacts New York City's data so what you'll see more broadly in the industry is that if a third-party private sector company has the data of New York City equities have been impacted, relevant victim notification will be sent out from that third party directly and, typically, depending on the provider, again, just industry trends, typically it's one to two years of identity services monitoring, for example.

CHAIRPERSON GUTIÉRREZ: Thank you. Actually, let me skip these.

I'll pass it to you, Council Member Hanif.

COUNCIL MEMBER HANIF: Thank you, Chair. Can you talk about the agency's cooperation with NYPD or lack thereof when it comes to assessing the cybersecurity of City agencies and the data they hold?

CHIEF MOAN: We have a collaborative relationship with NYPD. If you're speaking more broadly to cybersecurity threats, our partnerships with law enforcement doesn't stop at NYPD. It could also involve the federal sector to make sure that

they have insight into potential technical indicators that are available to make sure that other municipalities, other government agencies, other private sector entities aren't impacted by those same ongoing threats, and so when I reference cyber threat intelligence sharing, that's specifically what I'm referencing, and so that collaboration is omnipresent and that's not just for law enforcement, that's for private sector, our federal entities. Again, if we're seeing something, we're saying something about it to help in furtherance of the protection of those other sector entities.

COUNCIL MEMBER HANIF: So the collaborative relationship that you're talking about, what does that entail, or who is at the table for that?

CHIEF MOAN: Typically, it's security team to security team.

COUNCIL MEMBER HANIF: For agency?

CHIEF MOAN: For agency, but sometimes it extends even beyond that to IT teams, right? It depends on what we're seeing and who we need to loop in in furtherance of that protection and defense.

COUNCIL MEMBER HANIF: Who advises about the legality of the cybersecurity measures the City uses?

CHIEF MOAN: Legality of the cybersecurity measures?

COUNCIL MEMBER HANIF: In terms of determining what kind of technology, emerging technology, should be used over another.

CHIEF MOAN: So what I'm speaking about specifically is the cybersecurity tooling that is in place to protect and defend against cyberattacks, right, so that's best practices by industry. We have a defense-in-depth strategy, which promotes effective hygiene and cybersecurity tooling in addition to processes and procedures and cybersecurity awareness training to our City employees to make sure that we can thwart and attack it at any stage of the defenses that we do have.

COUNCIL MEMBER HANIF: And then are City agencies, including the NYPD, required to notify your agency about the tools they're using?

CHIEF MOAN: So like I mentioned before, we collaborate with agencies on both the cybersecurity tooling that they are leveraging. We

also provide those services to a large majority of them as well. We've unified in a number of different cybersecurity tools within the City. I can say that at a high level, because we immediately knew in the inception of New York City Cyber Command that there were tools that every City agency would benefit from, and so it made sense for both economies of scale and also autonomy to make sure that we have the appropriate protections in place such as endpoint security for every City agency to be able to take advantage of.

COUNCIL MEMBER HANIF: But it comes down to OTI in terms of sharing best practices and recommendations to each City agency.

CHIEF MOAN: Yes, we absolutely provide that advice, best practices and, in a handful of cases, we actually provide the tooling itself and, again, that benefits not just the agency, but us, and it's also been able to make us incredibly nimble and efficient in our services that we deliver, and it's also a method of a cost effectiveness as well to have that normalized baseline in place.

COUNCIL MEMBER HANIF: And then if a City agency has their own recommendations or they have a

tool that they want to use, does it have to be run by OTI?

CHIEF MOAN: From the cybersecurity perspective, we have the conversations with agencies who might be considering or thinking of something new that they want to purchase from the cybersecurity lens, and typically that conversation is a discussion about what the use case is and, if we already have something maybe in our tooling that the agency might not be aware of and, in some cases, it may not make sense for the agency to go out and do something on their own because we already provide that capability to them. They might not just be aware.

COUNCIL MEMBER HANIF: Got it. So just to get this straight, OTI works with City agencies to help determine what kind of technology they should use for their operations and, if they have a tool in mind that they'd like to use, you all collaborate on helping them understand if this is of good use, if this is the best tool for what they would like to use it for.

CHIEF MOAN: In the cybersecurity realm, for cybersecurity tooling is why in particular that I'm speaking about, yes. And I think that's important

because again, we have an ever-evolving threat landscape and, as those threats change, they might not realize we're also thinking about where we want to be in the next 5 to 10 years and what that ultimate cyber strategy is, and we often pilot new cybersecurity capabilities with our agency partners as well in addition to bringing them into the fold when we're looking at updating policies, procedures and the like.

COUNCIL MEMBER HANIF: And then the cybersecurity measures that these agencies use, is this public information?

CHIEF MOAN: Large majority of it is not. We also don't want to give threat actors a roadmap for what protections we do have in place. I will say that with regard to our cybersecurity program citywide, it is expansive and has core capabilities that you'd find in any well-managed and address cybersecurity program within even a private sector entity, and I think that's really what makes us unique and gives us an ability to have a chance at combating these threats that we're seeing on a daily basis.

COUNCIL MEMBER HANIF: Thank you.

CHAIRPERSON GUTIÉRREZ: Thank you, Council Member Hanif.

I just want to jump back to just a followup on the previous question regarding who bears responsibility in the event of a cybersecurity incident. Can you share if Cyber Command has activated any vendors insurance coverage policy following a data breach or credit monitoring?

CHIEF MOAN: Off the top of my head, I can't speak with 100 percent assurance, but I do know that in the past, in regards to victim notification in particular, typically depending on the vendor, we have seen victim notification be delivered through a vendor or a private sector entity that hasn't bared a cost to the city, right, so that has been directly from the private sector entity to the victim itself via letter, the relevant victim notification process that you find.

CHAIRPERSON GUTIÉRREZ: And in the example of victim notification, are those pieces of like the agreement or policy that OTI works through in every specific agreement or contract, excuse me? I guess how do we know in those instances when the vendor's

insurance policy is going to be utilized for something as important as victim notification?

CHIEF MOAN: Great question. The cyber insurance landscape has also continued to evolve even speaking more broadly in the private sector realm over the last few years, especially with very well-known and high-profile attacks that have hit private sector companies. Typically, again, just speaking from my experience and background, typically when a private sector entity endeavors to get cyber insurance, typically that policy does include provisions for victim notification and the relevant costs to that. I'm not a 100 percent authority, I'm not a cyber insurance lawyer nor a provider, but I do know that large in part that is why we have the cyber insurance requirements for our vendors as well, so that they have that backstop too.

CHAIRPERSON GUTIÉRREZ: Thank you. Can you share a little bit about cloud riders? I know in your previous responses, it's not necessarily your unit that works on reviewing cloud riders, but it is kind of like a multi-unit process within OTI to review every agency's cloud rider. It's my understanding through the cloud rider that every vendor must submit

an annual audit of their privacy and security programs to the City. Did your agency review this audit before MOVEit was adopted into New York City public schools?

CHIEF MOAN: MOVEit, in particular, was a zero-day vulnerability that did not provide a fix upon disclosure, and so the nuance there, and for folks, again, who might be listening in, MOVEit is a file transfer solution that was used at an impacted agency and publicly disclosed, again, want to reiterate that this is in the public domain so I am able to speak about it a bit more broadly. In the case of MOVEit, unfortunately, our City agency was one of hundreds of victims that were impacted by a zero-day vulnerability that was taken advantage of by a threat actor prior to even disclosure, and so I want to reiterate that because, again, we have a strong third-party risk management strategy, multiple layers of not just our internal controls but also managing those from outside of the City domain perspective but, in particular, the case of MOVEit, the software had a flaw that was not known to MOVEit or the agency and, ultimately, the threat actor was able to take advantage and exploit that

vulnerability, leading to hundreds and hundreds of victims, not just government entities but also private sector entities as well, and so while we have, for example, cloud services agreement, although MOVEit was not a cloud services solution, that we have provisions in there specifically to provide us notification in case there's an incident that's being suffered at a third party so that we're aware of the incident and we're able to ask questions and attempt to curtail any impact to New York City as that incident transpires.

CHAIRPERSON GUTIÉRREZ: Okay, I have a few more questions. I think we're almost there to public testimony.

Regarding citywide cybersecurity protocols, how often does OTI review and update those policies?

CHIEF MOAN: Periodically. Just this year, we updated our internal password policy, which was a lot of hours and a lot of hard work to make sure that we're balancing both the new and emerging landscape of passwords but also our agencies as well so that's just one example of many.

CHAIRPERSON GUTIÉRREZ: They're reviewed periodically, but are they updated?

CHIEF MOAN: They're updated periodically as well.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF MOAN: We have a policy team that reviews and updates where necessary for new tactics, new processes that are in place or just, again, that the technology or the cybersecurity industry has changed tactics or approach on a certain matter, making sure that we're building new policies to impact.

CHAIRPERSON GUTIÉRREZ: Do you know if the updates are publicly available?

CHIEF MOAN: So a lot of our policies, rightfully so, are only available internally. We also have a subset of policies that are made available publicly and typically updates as they're made internally to the internal policies and standards and guidance, the relevant updates to the public-facing site would be made as well.

CHAIRPERSON GUTIÉRREZ: Okay. What we looked at was at, we were not privy to any updates since the last Administration, and it's probably

because it's not publicly available, and I know, pursuant to Local Law 89, Cyber Command must regularly update these policies. Is there a way that it can be made public or that it can be shared, or how can we, the public, know or trust that OTA is following this law?

CHIEF MOAN: Absolutely. You ask a great question. I would endeavor to offer an opportunity to discuss with your office and this particular Committee more broadly about what that might look like. We obviously want to strike the balance between public awareness that, yes, it is absolutely normal and routine for us to be periodically updating policies and frameworks while also not wanting to reveal too much internally sensitive security documentation that would lead threat actors to be able to perpetrate attacks against the City so I think that that's definitely something that we would be open for discussion.

CHAIRPERSON GUTIÉRREZ: Okay. Does Cyber Command conduct regular audits of agency cybersecurity readiness and responsiveness?

CHIEF MOAN: So we have a number of different work streams that we engage with City

agencies, including on response and readiness, in addition to assessments, and we also sometimes have, in addition to that, third-party audits that are taking place throughout the City as well that we're closely partnered on.

CHAIRPERSON GUTIÉRREZ: Okay, let me fast forward. I want to ask more specific questions about some events regarding DOE and MOVEit. Those affected by the data breaches from MOVEit software and Illuminate were apparently not notified until weeks after these incidents transpired. Could you detail for the record the timeline there and why it took so long for affected parties to be notified?

CHIEF MOAN: Sure, so MOVEit was a zero-day vulnerability that was exploited last summer very quickly upon disclosure of the vulnerabilities globally, and we partnered with DOE to ensure relevant mitigations were put in place. Unfortunately, very quickly after, we identified, again, in close collaboration with the DOE team that there was a cyber incident that had taken place and the threat actor was able to exploit information. Approximately 19,000 unique files were exposed and so, upon identification that relevant files were

exposed, the process started to identify what, if any, sensitive data elements were potentially exposed as part of those files so that analysis, we partnered closely with a leading e-discovery firm to do that analysis of line by line by line to determine what data elements were impacted, and that was in close collaboration with the agency privacy team and the Office of Information Privacy.

CHAIRPERSON GUTIÉRREZ: Thank you, and what can you share about the timeline though? How soon after was OTI notified and what was the lapse of time between when you were made aware and then the…

CHIEF MOAN: So if I'm remembering correctly, it was, I want to say, roughly between 60 and 90 days from all…

CHAIRPERSON GUTIÉRREZ: Six to eight days?

CHIEF MOAN: 60 to 90 days from the determination that there was a disclosure of the vulnerability, right? Not a fix, but the global community identified and were made aware that there was a vulnerability to a full accounting from the DOE and e-discovery team of the relevant victims and those notifications being shared with what data elements were then impacted.

CHAIRPERSON GUTIÉRREZ: Is there any way looking back now that Cyber Command could have helped in this process in at least notifying the affected parties in less than 90 days, potentially?

CHIEF MOAN: So in the particular case of MOVEit, we actually worked incredibly quickly more broadly but also in comparison to others that were impacted. If you take a look at what's in the public domain about other entities that were impacted and associated timeframes, we are on the faster side and, in particular, the investigation itself from initial disclosure of vulnerability to identification of unauthorized access to 19,000 unique files was quite quick from a cybersecurity perspective and that's what we endeavor to do each and every time. A sense of urgency is incredibly critical to making sure that we can affect notification should it be relevant as soon as possible. The actual act and, again, I'm not sure how much folks know about how the sauce is made from a analysis perspective, but the analysis to determine if a data element was impacted is quite complex and making sure that we had the totality of data that was impacted and tying that back to individuals was a paramount consideration for the

City, making sure that we were full and all-encompassing and that meant multiple layers of reviews and assessment with our e-discovery firm and, when I say we, I mean DOE and New York City Cyber Command in addition to the privacy teams as well.

CHAIRPERSON GUTIÉRREZ: Thank you. Can you discuss what you know about the incident involving the New York City Law Department and how would you classify it? I just want to be mindful of the proper terminology.

CHIEF MOAN: So, as I understand it, the New York City Law Department suffered an incident in 2020, I believe. Although I can't speak to specifics of the particular incident details, I do know that we work and continue to work collaboratively with Law Department to enhance and continue to increase cybersecurity maturity as they are just one of many agencies that we do this with and that is routine and commonplace in nature that we have these conversations with our agencies.

CHAIRPERSON GUTIÉRREZ: Can you share about anything specific that happened in that compromise, in that incident?

CHIEF MOAN: Unfortunately, I'm not able to at this time given the public nature of this session, but I am happy to offer up a discussion offline.

CHAIRPERSON GUTIÉRREZ: Okay. I want to wrap up with something that we've spoken with to OTI directly about the NYCAPS Employee Self-Service issue, and I just want to say that I think from the time that we were notified to the time that the site was accessible outside of work computers, I think that was very quick so I just want to acknowledge that much, but there were a lot of questions and that brings us to kind of the protocol in notifying us as the Council, yes, but as also people that utilize this service like myself. This was during tax season. I personally found out through the news that there was no direct notification. I think the direct notification from OTI came maybe 24 hours after it was dropped in the news so I just want to ask if you think there were aspects of OTI's response to that cybersecurity incident that you believe were important in areas that you think can be improved.

CHIEF MOAN: Thank you for the question and, again, thank you for allowing me an opportunity

to speak about this publicly. I think a couple things are really important to just provide the public an overview on.

First, as I mentioned in my opening and continued thread, social engineering tactics, tactics to lure individuals to disclose their sensitive information or their credentials continue to be omnipresent as a tactic being used by threat actors and so, in this particular case, we worked expeditiously to identify, to close any threats that were ongoing that users might have been susceptible to. In the particular case of ESS, we also identified that there could be an opportunity to improve cybersecurity hygiene in furtherance of protecting users. As I mentioned, users are a line and our City workforce is a significant line of defense against cyberattacks, which is why we have a robust cybersecurity awareness and training program, but the reality is is that I think we all in this room and online probably have either yourselves suffered from a cyber incident where you're disclosing your username and password or somebody in your family, somebody that you know and so, it was really important for us to work with FISA and DCAS to very

rapidly identify that there was an area of opportunity. We could take advantage of the timeframe of identification of a threat, and we worked quickly to implement enhanced security measures in the public facing portal, and we did so because we believed it was the right thing to do and we did so quickly with close partnership, obviously with FISA and DCAS.

In terms of communication, just like any incident or any routine business that Cyber Command endeavors to enter into, we always are looking for ways to improve and be more efficient and optimize. I think my team hears that from me about 50 times a day. In that regard, I think communication for a citywide base, right, we have relevant communication procedures with our security teams with HR teams, IT teams, and all of that is well-actioned and well-understood. In this particular case, we took an above-and-beyond action for our public facing portal to implement enhancements and, with that, coincided with an engagement and awareness campaign that really had never been done in totality across the City base.

CHAIRPERSON GUTIÉRREZ: Sorry. There was a public awareness campaign on this particular, on the Employee Self-Service site?

CHIEF MOAN: Within the City domain, yes.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF MOAN: And so that was new and novel for that to be done, and I think that's important to mention because as we see more tactics being perpetrated by threat actors but also an opportunity to double down on the messaging that you as an individual are a line of defense and essentially a human firewall, as we call it, against these attacks, it’s also important to socialize that citywide and so, with partnership with DCAS, we were actually able to send out a threat alert for agency employees, even though that ongoing threat for that particular threat actor was neutralized. We still thought it was to the benefit of the population in the community that we were able to send out that alert, and so, as part of any incident, there's always an after action, areas of opportunity that we can enhance and that we can improve and, while it is never a good day when we suffer an incident, it always provides an opportunity of improvement and maturation, which continues our cybersecurity journey and posture for the city.

CHAIRPERSON GUTIÉRREZ: Can you share how many City employees were directly impacted by that incident?

CHIEF MOAN: So what I can share is a very, very small number from what we know, incredibly small number, and that's in large part, and I have to give a kudos to my team who's able to neutralize the threat, the ongoing threat, very rapidly from identification that there was an ongoing campaign targeting New York City to being able to neutralize that threat, although there were a handful of City employees that did disclose their login information.

CHAIRPERSON GUTIÉRREZ: And we were made aware that some City employees have received mandatory cybersecurity training that was issued by a third-party vendor. Is this standard practice and are there any plans to create that cybersecurity training in-house?

CHIEF MOAN: Oh, so our cybersecurity awareness and training program, that might be what you're referencing. It is very routine to leverage platforms to actually push out content about the training. It's also very normal for, and our team does it, to create custom content to then push out to

our City workforce, especially contoured or developed around certain initiatives that we're focusing on. So typically, Cybersecurity Awareness Month, October is a huge month for us, right before the holiday time where we know that folks are susceptible, even in their personal lives, of being taken advantage of from a social engineering perspective so we oftentimes send out a ton of programming around how to protect yourself online. When we implement new security capabilities or methods to, let's say, report phishing, we are also able to, and we have, create custom content that targets engagement of that specific capability or practice that we're trying to train users about.

CHAIRPERSON GUTIÉRREZ: And did you share the name of the vendor?

CHIEF MOAN: We typically don't share the name of the vendor. I'm happy to offline but, again, regardless of the vendor, it could be any vendor that provides a platform to disperse the training. The content and the key themes that we are focusing on, like multi-factor authentication and how to report a phish is all pertinent to the city of New York.

CHAIRPERSON GUTIÉRREZ: I want to acknowledge Council Member Julie Won, who's just joined us.

My last question is on Intro. 539, which is prohibiting third-party sale of geolocation data. I know you spoke to it in your testimony about enforcement, not really being an OTI's responsibility. Would you be able to share which agency you think this bill would more accurately fit under?

CHIEF MOAN: Off the top of my head, I'm not able to share in specifics at this moment. I do think that conversation and discussion with the Committee is something that we would absolutely like to have, we're happy to have, and it would significantly assist in being able to answer some of the questions that we've got.

CHAIRPERSON GUTIÉRREZ: Thank you, yeah, I look forward to it.

Okay, well, thank you both. I feel like that was a marathon. That's great.

I now want to open the hearing for public testimony. I encourage you all to stick around if you can.

I remind members of the public that this is a formal government proceeding and that decorum shall be observed at all times. As such, members of the public shall remain silent at all times.

The witness table is reserved for people who wish to testify. No video recording or photography is allowed from the witness table. Further, members of the public may not present audio or video recordings as testimony, but may submit transcripts of such recordings to the Sergeant-at-Arms for inclusion in the hearing record.

If you wish to speak at today's hearing, please fill out an appearance card with the Sergeant-at-Arms and wait to be recognized. When recognized, you will have two minutes to speak on today's hearing topics on Cybersecurity and Intro. 217, 425, and Intro. 539.

If you have written statement or additional written testimony you wish to submit for the record, please provide a copy of that testimony to the Sergeant-at-Arms. You may also email written testimony to testimony@council.nyc.gov within 72 hours of this hearing. Audio and video recordings will not be accepted.

Our first panel, we have Albert Fox Cahn, Shane Ferro, and Nina Loshkajian. I apologize, Nina.

Okay, thank you all, thank you for waiting. You all can begin, whoever wants to start.

NINA LOSHKAJIAN: Hi, thank you. Good afternoon, Chair Gutiérrez, Members of the Committee on Technology. I appreciate the opportunity to testify today on the harms of biometric surveillance. My name is Nina Loshkajian, and I am a Staff Attorney at the Surveillance Technology Oversight Project.

CHAIRPERSON GUTIÉRREZ: Nina, I'm apologizing for mispronouncing your last name.

NINA LOSHKAJIAN: And I'm here to urge the Council to pass Intros 217 and 425, banning public accommodations and landlords, respectively, from using facial recognition and other creepy biometric tracking tools. Facial recognition is biased, error-prone, and harmful to marginalized communities. In our eyes, the legislation in consideration today is largely a mirror of existing civil rights protections. We don't allow stores and landlords to discriminate on the basis of race, so why do we let them use racist technology? Simply put, these systems have no place in New York City homes and New York

City businesses. These measures are an indispensable safeguard, but we also implore the Council to go farther and introduce legislation banning law enforcement and government use of biometric technology. Even if the algorithms could be improved, biometric tracking would remain just as discriminatory because of the ways the creepy stalking tools are plugged into discriminatory policing, housing, and commercial practices. BIPOC tenants and shoppers will not be given the same benefit of the doubt as white tenants and shoppers when faced with a facial recognition error, and I also wanted to flag, so I believe it was Council Member Paladino who expressed concerns about co-ops, it's important to flag that Intro. 425 only applies to owners of multiple dwellings trying to identify tenants, so I don't think actually this bill would address co-op boards. This is about renters in particular. But back to places of public accommodation, New Yorkers should not be forced to accept constant tracking as part of simple activities like buying groceries or taking their kids to a baseball game. Stores biased facial recognition systems will exclude black and dark-skinned people

due to incredibly common mismatches. I think Council Member Hanif was right earlier to flag the Rite Aid example. The FTC saw how dangerous it is when stores use this technology, and that is why Rite Aid is now banned from using it for five years. It is also crucially important that these technologies stay out of our homes. Without legal intervention, the collection of biometric data will affect not just residents but guests they have over and, in particular black, brown, Asian, and gender-non-conforming guests will be barred from visiting their friends due to mismatches as well. In New York City public housing, facial recognition use has already led to residents being evicted for minor violations of policy, and this will contribute to the city's massive eviction crisis. Vendors of this technology have been clear about their intentions. They have stated that they would like to find loopholes to be able to charge tenants more on rent using this technology, and I'll wrap up shortly, apologies. We do encourage the Council to consider one important addition to the bill, banning this technology in residences which is a strong private right of action to make sure that tenants have a way to hold their

landlords accountable and, as I mentioned, we also encourage the Council to consider a ban on government use and law enforcement use. Thank you so much for your attention to these issues.

CHAIRPERSON GUTIÉRREZ: Thank you, Nina. I have a question, but I'll wait for the panel here.

ALBERT FOX CAHN: Good afternoon, Chair Gutiérrez, Members of the Committee. Thank you for the opportunity to testify. My name's Albert Fox Cahn, and I'm the Executive Director of the Surveillance Technology Oversight Project, and I am offering written testimony in support of Intro. 539 today which would prohibit the commercialization of our location data which is a routine part of how New Yorkers are being tracked every single day, having our devices turned against us as a way to market to us, to sell products to us, sometimes even police us. We see this data being used by law enforcement. We see this data being used by even government agencies like the IRS. In our testimony, we spell out why it is so important that New York City fill the regulatory gap that has been left by Albany, that has been left by Washington, that has left New Yorkers exposed to having their most intimate moments

collected by an unregulated wild west of apps that are constantly churning out new and horrifying ways to turn our every single moment, the record of how we live our lives into a product for the highest bidder. This is something that New York can take a leading stance on where we can be on the cutting edge and, as we point out in our written testimony, there is one change that would be helpful adding a clear carve-out for defense attorneys in criminal investigations to make clear that criminal defense attorneys, like police officers, operating with a warrant have the ability to obtain this information from these companies because no one should be denied a defense in court because of this privacy protection. This should be a way to protect us from this sort of dragnet surveillance, but I think I want go back to the City's kind of shocking testimony more broadly because we heard from agencies that this City is on the cutting edge of protecting New Yorkers and that they are absent. They are completely absent from the issues that brought us here today. They're absent from talking about biometric technology and they put forward a false question. This false debate about privacy versus security because what I'm here to tell

you today is that this technology poses a threat to the public and offers us nothing in return. This technology is ripe for abuse and exploitation, and this isn't protecting us from acts of terrorism at Madison Square Garden, it's protecting Dolan from critics and litigants at Madison Square Garden. It's protecting his ability to control a public space as a private fiefdom, and that's the sort of abuse we see with these sorts of technologies, the largest companies abusing it every day to target New Yorkers, and that's the sort of power imbalance we shouldn't allow to continue for one day longer.

CHAIRPERSON GUTIÉRREZ: Thank you, Albert.

SHANE FERRO: Good afternoon. Chair Gutiérrez, the rest of the Committee. My name is Shane Ferro. I'm a Staff Attorney at the Legal Aid Society in our Digital Forensics Unit. My job is to fight for the civil liberties of our clients and, by extension, all New Yorkers in the face of exponentially increasing uses of digital surveillance. The use of biometric surveillance and especially facial recognition in public places erodes any right to privacy we have as citizens, diminishes our civil rights, and reduces our democratic values.

It's especially important in a city as large as ours that we protect the rights of people to move freely without worry that every movement they make could be tracked. Every person has a right to privacy and autonomy and whatever small amount of space they're able to call home. Biometric surveillance, particularly facial recognition technology, is built on top of and perpetuates historical racial biases. That is why so often it doesn't work on black faces and why almost every known cause of false arrest as a result of facial recognition has been of a black individual. It's unconscionable to allow private businesses to discriminate against community members and customers using what we know to be biased and racist technology. It's also, quite frankly, creepy to know that every business that you walk into or walk next to on the sidewalk might be able to know who you are and track your movements just because you walked inside or outside the door. Unfettered facial recognition use doesn't just harm the people it misidentifies, it also subjects every citizen to massively increased surveillance. We must reckon with the significant harms the City has inflicted on its poorest members through its housing system. We have a

published well-known list of the City's worst landlords and regularly see stories of large private landlords who refuse to do repairs and try to push out longstanding tenants to jack up the rent. Yet vacancy rates are in the low single digits, and a huge amount of our city's residents have very little leverage over their landlords if they want to be able to continue to live here. A huge swath of our city has little autonomy or control over their own private residences. We should ban further eroding their rights by subjecting them to any type of biometric surveillance to get into their own homes. There is a concept in American law, the reasonable expectation of privacy. It's currently the core of our democratic and civil rights under the Fourth Amendment. The more that biometric surveillance is allowed to permeate every space that our citizens exist in, the less society can rely on any expectation of privacy being reasonable. When there's no longer any place that a person can expect to go, not their apartment, the grocery store, the pharmacy, not a basketball game, without their face being captured, indefinitely stored in a database, and constantly checked against suspicions of having done something wrong, then we've

hollowed out any shred of hope that a person can expect, reasonably, privacy or democratic values anywhere. I don't want to live in that world, I don't want my clients to live in that world, I don't want my community to live in that world, and I hope you don't want to live in that world. Thank you.

CHAIRPERSON GUTIÉRREZ: Thank you, Shane. We have some questions.

So it's hard for me, obviously, as a sponsor to both bills, but it's really hard for me to grapple with where a space for facial recognition technology can live safely in our city, let alone City government. The Administration was obviously not equipped, or, I don't know, was not prepared to answer questions. We know which agencies are using biometric information. Unfortunately, we learn of this when it's far too late, oftentimes when these folks are already in the criminal justice system, so I was disappointed, but are there any positive examples of where the use of facial recognition technology is beneficial?

ALBERT FOX CAHN: I would say there's a world of difference between the facial ID we use to unlock our devices and the facial profiling that

tracks New Yorkers in public spaces. It's about power, it's about consent. When we use this as a tool to unlock our own device, that is a very different question than when these unaccountable companies and institutions weaponize our own bodies against us and use it as a way to track us in public spaces so that's why these bills wouldn't impact your ability to use this sort of biometric identifier on your own device as a way to unlock your own data, but that's not the sort of thing that people have ever been pushing back against.

CHAIRPERSON GUTIÉRREZ: Thank you. I'm going to pass it to Council Member Hanif, but I just wanted to ask questions on Intro. 539, which is the first time that we're technically hearing this bill on geolocation data. Can you share what types of location data you all are most concerned about?

ALBERT FOX CAHN: I mean, when we think about location data, we think about nearly everything we do. If you go to a political protest, if you go to a house of worship, if you go to a reproductive healthcare facility, if you go to your kid's school, and any sensitive site we go to in our lives is up for grabs for the highest bidder, and it's not just

something that we see being routinely weaponized by law enforcement, but it's also something that we see being used by political extremists, that can be used by any number of groups. It's really cheap, right? It would just take a few hundred dollars to get the geolocation data of everyone in this room right now, to get a data set that we could then use to track where people go throughout the day, how they're living their lives, what other places they go to and, to me, this really does go to the heart of what it means to be a democracy. We need to be able to have the capacity to go places without second-guessing how that's going to be weaponized, and this is something where we've seen regulators in Europe really taking these privacy concerns more seriously but, right now, we see this huge market in the U.S. for data brokers that will sell this information seemingly to anyone and, really, it's something that I'm glad to see the City taking a leadership role in pushing back against.

CHAIRPERSON GUTIÉRREZ: Do law enforcement agencies buy location data?

ALBERT FOX CAHN: Oh, yeah.

CHAIRPERSON GUTIÉRREZ: Or get it handed to them?

ALBERT FOX CAHN: At Surveillance Technology Oversight Project, we're currently suing Thomson Reuters which sells the personal information of nearly every single American to dozens, maybe hundreds of different law enforcement agencies, including immigration officials. Data brokers are fueling deportations. They are one of the major tools used by those officials, but it's also being used by cybercriminals and used by hackers. It's used by any number of people to break the law as well as the police departments that so often abuse it so, to me, it's kind of like we've left some of the most valuable assets we have as a society just completely unprotected on the market for whoever wants to take them.

CHAIRPERSON GUTIÉRREZ: My last comment/question is, I think oftentimes in these spaces, for folks who support the use of biometric data, particularly with law enforcement agencies and PD, they'll kind of put the onus on the user, right? Like, well, it's in the terms of service. Who, I can't tell you the, I mean, you know what I mean,

like the reality of people reading through pages and pages of terms of service. Is there something else? I know, obviously, these bills are a reflection of that, but is there something else that we can do where the onus isn't on us? Is there something that we should be requiring these individual companies, agencies even, to require more consent, opting in, knowledge? Oftentimes, I don't think that people understand that the terms of their service agreement is that, is allowing to share your information with nobody you'll ever know, no third party you'll ever understand. Is there anything else that other localities are doing? Is there anything else that we can do? Then I'll pass it to Council Member Hanif.

ALBERT FOX CAHN: I mean, look, as a privacy lawyer, I think of terms of service as just a shared lie that we buy into this façade that people are going to actually go through and read these terms, that they're going to understand these terms, that they're going to consent to it. No one reads them and, even if you do read them, even as a lawyer, I rarely could actually understand them, and so I think anytime we're putting the onus on people to sort of make these truly, sometimes life-altering

decisions about what data is made accessible to other people in the fine print of a menu that they download in some free weather app or some free traffic app, to me, that is a broken system, so I think we need structural protections that ban the commercialization of our most sensitive data, that shut down this massive market in selling our location data to the highest bidder, and that really just start to outlaw some of the most abusive forms of facial recognition and other biometric data collection, and say that we should never be putting someone in the position that they're one mouse click away from wiping away all of their privacy protections.

NINA LOSHKAJIAN: Can I add briefly to that? Because you talked about it in your question, the PDU specifically. There's also a lot of requirements that the NYPD is currently under that they're not complying with under the POST Act. They're failing to comply with the very…

CHAIRPERSON GUTIÉRREZ: They don't use facial recognition technology is what they say, is what they said.

NINA LOSHKAJIAN: Well, they don't use it as a sole basis for arrest, but then, you know, so

their IUP on facial recognition is boilerplate language so holding their feet to the fire in terms of actually asking them to comply with the minimal requirements of things like the POST Act, that's another thing you could do, we could explore, and there is also different legislation on this, but we could explore more requirements before deployment of this technology because oftentimes we'll find that after this biometric tracking is already pervasive, the harm has already been caused, and it's too much to ask them to do anything after the fact so just to address kind of PDU specifically, actually requiring them to comply with the current law, to comply with FOIL because we've also been litigating to get information from them for years and years about how they use facial recognition, so those types of things are also avenues to explore.

CHAIRPERSON GUTIÉRREZ: Thank you. Council Member Hanif?

COUNCIL MEMBER HANIF: Thank you, Chair, and thank you for your testimonies. Humans recognize people by faces. That's one of the main jobs of a door attendant. Why shouldn't a computer do the same thing?

NINA LOSHKAJIAN: Because it's not as good as it, and it's been trained only to recognize certain types of faces. The algorithms that facial recognition systems use and rely on, I think it was Council Member Paladino again who said that they are 99 percent accurate. That is true only for white men under ideal laboratory conditions. For women of color, they can be like less than a third accurate, so the discrepancy is between the pool of people that these tools were trained on and real-world conditions that they're being deployed in now are just night and day, and I don't know if the other panelists want to add.

SHANE FERRO: If I could also add, facial recognition is something of a misnomer. Recognition is like a human thing. As you got out in your question, what these algorithms do is not actually recognition in any real sense. It's mathematics and algorithm. It's a matching system, and that match can never be 100 percent accurate. A computer can never recognize a person. It can only say that it maybe matches a face that's within the database, and we know that those matches are often inaccurate.

COUNCIL MEMBER HANIF: Can you respond to just the climate of fear that we've seen both the last time this was heard and now that there's a rise in shoplifting, there's just a rise in crimes. How do you respond to that when it comes to biometric surveillance and just public safety in general as we try to protect our city's businesses?

SHANE FERRO: Yeah, I mean, it's a really frustrating situation to be in because we keep seeing this pattern that a convincing story is far more powerful than the truth in many cases because what we saw over the last few years was bad data being put out there by retail federations that were claiming there was this massive surge in organized shoplifting and it got all this coverage and we saw news reports on it, front page stories, we saw all these evening news clips, and then it turned out it was wrong, that they had screwed up the data, that there wasn't an increase, but you couldn't unbake that cake. You couldn't make people unsee all of those stories they had seen and, because of that bad data, we had this just sense that there had been a just awful reality unfolding, not one we saw personally, because it didn't exist, but one around us, that maybe it was

impacting our neighbors, maybe it was a store down the street, and so you have this fabricated sense of fear built on bad crime stats, just creating this fertile ground for the surveillance salesmen to come in and say, oh, if you have this tracking tool, if you collect this data, you'll be safe. Do we have data to prove it? No. Do we have evidence to support it? No. Has it been disproven over and over again? Sure, but don't look at the facts. Just, you have that sense of safety. And so for the people who are working at businesses, who own businesses, who are afraid, who are trying to keep their staff safe, my heart goes out to them, because I know that's not easy. I know there are real things that you can do to improve the safety of your store, but the truth is, they're getting sold a bill of goods. The cameras don't work. The facial recognition doesn't work. They don't reduce theft. They don't do the things that we've heard over and over again they're helpful for and, quite frankly, we have several decades of evidence that mass deployment of CCTV cameras is one of the least effective ways of preventing crimes. This goes back to London's mass deployment of CCTV during the ’80s and ’90s, but people feel safe, so

they invest in it, and so what I just want to say is, it feels good for some people to have that camera, they have that illusion of safety, but the reality is it's a threat to a lot of the people who walk into that store, and the reality is it's very rarely, if ever, going to keep anyone safe.

CHAIRPERSON GUTIÉRREZ: Thank you, Council Member. I have some more followup questions. Is it possible for someone to be removed when someone's biometric information has been captured? You referenced this very specific moment during the pandemic, and I know I personally spoke with business owners that were really relying on this technology for the reasons that you've highlighted about how this is an inaccurate system, would I be able to remove my image from this cloud of data that exists with my biometric information? In the same way that if you were on PD's gang database, you're on it for life, if you're associated with someone, you're on it. What recourse does someone have here? Are they even made aware that their information obviously is being captured, but can someone be removed from, I guess, data recognition collection? If it's possible, I'm honestly asking.

ALBERT FOX CAHN: The first problem is you usually don't know when you're in one of these databases, the second problem is they don't actually have an opt-out or removal mechanism, and the third problem is that all of this data is constantly being proliferated from one database to the next so, even to the extent that you somehow found out someone was using this facial recognition system and you asked them to remove it, that's not a guarantee that your data hasn't already migrated somewhere else, and it's really alarming with biometric tracking that this data is being collected because if your credit card gets stolen, you can change your credit card number. If your identity is stolen, it's a pain, but you can even change your Social Security Number. But if your biometric data is compromised, if someone is accessing your biometric data to impersonate you, there's nothing you can do because that's going to be your biometric data for the rest of your life. You can't change your face. You can't change your fingerprints, and so there's a real persistent harm, and I just think that with all of these systems, it's kind of unnerving to me how, even though in New York City it's been law for quite some time that any store

using biometric surveillance needs to publicly post that, needs to tell people, needs to give them that notice, we still hear lots of reports about large companies that are doing this, and we're currently in court against Amazon and Starbucks amongst others for allegedly taking New Yorkers' biometric data without the sort of notice and consent that's required under City law.

CHAIRPERSON GUTIÉRREZ: Regarding both 217 and 425 and a little bit with the POST Act, Mayor Adams announced that PD is expanding an initiative allowing businesses to feed security camera footage to PD. You referenced this as an effort to curb shoplifting. We've heard at our POST Act hearing last year that PD does not use live facial recognition. Do you have any concerns about this new initiative? Nina.

NINA LOSHKAJIAN: We have many concerns because, I mean, like Albert mentioned, I mean, there's so many… First of all, we have to take them at their word that they don't use live facial recognition. We don't know if that is actually true, and this kind of live streaming from, for example, if your grocery store starts using facial recognition,

under the current law, they would be required to post that they are but, if the new agreement, new state of play becomes that your grocery store just has a surveillance camera and then that stream is being fed to the NYPD and then the NYPD is performing facial recognition, does that mean that customers don't need to be notified under the current law? There's all sorts of concerns that we have about this new dynamic that would come into play, and also that means that there's no opportunity for people on the ground. This could mean that NYPD just automatically deploys officers because of a mismatch that said, oh, there's a shoplifter in X store. That will unnecessarily lead to a violent interaction. Whereas, obviously we oppose this technology use in general, but with stores just using surveillance cameras, they can be monitoring those, and then they can go see what's actually going on, or they have kind of, a lot of business owners say they know the repeat offenders, who they actually are like human recognition, so there's just a whole new dynamic that will come into play if there's that kind of live stream to the police.

SHANE FERRO: I would also add that even if they aren't using facial recognition, they may be using sophisticated video analytics such as object recognition, which allows them to basically surveil thousands of video feeds live at one time and have algorithms that identify suspicious objects, quote unquote, that they then turn their attention to that, and so the video analytics is basically doing the job of thousands of officers watching screens at one time, meaning that they can search through and find certain things even without it being a face in a way that is, again, very creepy, and that has not been explored as much as facial recognition.

ALBERT FOX CAHN: I mean, to me, this is the latest example of a Mayor that prioritizes public relations over public safety. He always wants to find the high-tech gimmick that supposedly is going to keep us safe, but how many cameras do we actually need, all right? We see tens of thousands of cameras that are owned and operated by the NYPD, tens of thousands of cameras that they access through the domain awareness system on top of that. We see this new pilot product so how many cameras are going to supposedly keep us safe? To me, it's really just this

constant effort that whenever there's something about crime in the news, the Mayor will say this expanded program will somehow work without ever providing any evidence that the past camera systems have lived up to the amount of investment we've made in them, and I will say, looking at the disaster that Detroit has had and that several other cities have had with similar public-private camera partnerships, it's really alarming because in Detroit, under their Project Greenlight, there were allegations that stores were being coerced to agree to this sort of partnership, being told, hey, you're going to get faster 9-1-1 response if you sign up to this thing versus the other folks who don't and so, again, there's a lot of potential for abuse and a very questionable premise that this is helpful at all.

CHAIRPERSON GUTIÉRREZ: Thank you. I have one more question before I pass it to Council Member Holden.

We came across that Maryland recently enacted their digital privacy law that prohibited the use of geofencing near mental health facilities and reproductive or sexual health facilities. What is your opinion of that more targeted approach here?

ALBERT FOX CAHN: We don't think that a targeted ban on geolocation data collection actually can be effective at protecting people who go to those facilities compared to a blanket ban on geo warrants and those sorts of mass geolocation tracking or the type of bill we see with 539 because when you simply have those more narrow protected facilities versus the broader ban, you'll just see gaps in people's location history which can be indicative of the fact that they went to just such a facility, and there was a lot of pushback against Google when they initially responded to the Dobbs decision by limiting the geolocation collection around those sensitive sites, and it also turned out it was really hard to implement and so Google eventually moved completely to device side data storage as a way to respond to that issue because they found that they couldn't consistently operationalize those more targeted limitations.

CHAIRPERSON GUTIÉRREZ: Thank you so much. I'll pass it to a Council Member Holden for questions.

COUNCIL MEMBER HOLDEN: Thank you, Chair, and thank you all for your testimony.

I just have some questions on camera use. Let's say this our legislation today prohibiting facial recognition from businesses and let's say they have the software. How do we enforce that law? I mean, what do we do? Go into the, let me see your software, what do we do with that?

ALBERT FOX CAHN: Well, I'm currently litigating a case against Amazon for exactly that issue where they were using biometric data collection according to our complaint that violated New York's law because they weren't disclosing it, and we observed the camera placement. We observed the type of software they were using, and we were able to file a complaint in federal court, and I think that we…

COUNCIL MEMBER HOLDEN: Well, no, just one, how do you determine the software they're using? That's what I, from Amazon. Did they disclose that?

ALBERT FOX CAHN: We were able to look at the models of cameras that were installed, the layout of it, public documents from the company.

COUNCIL MEMBER HOLDEN: But still, you didn't know for a fact.

ALBERT FOX CAHN: No, we…

COUNCIL MEMBER HOLDEN: You're looking at the placement of everything.

ALBERT FOX CAHN: No, we had documents from them as well. I would say when you look at analogous laws, like the laws that enable you to sue a store that has discriminatory construction for non-compliance with the Americans with Disabilities Act or are suing a venue that has other discriminatory technology, there's always the pre-litigation fact-finding phase, but that's something we have a really strong model for and also we know that there are employee whistleblowers, there's disclosures to law enforcement if that information is used in an arrest that can come out during discovery so I'd say there's a lot of robust mechanisms.

COUNCIL MEMBER HOLDEN: All right, but you're, can I just finish?

You object to the facial recognition because it's an invasion or because it's not accurate. What's the main thrust against that facial recognition? Let's say they reached 99.9 percent accuracy for everyone. Would you still be against it?

NINA LOSHKAJIAN: Yes. As I mentioned in my testimony, even if the tool itself is 99 percent

accurate, it will be plugged in to systems that are discriminatory in housing, in public accommodations and, as Shane mentioned, that's just not the world we want to live in that you are tracked every single place you go. We just don't think it's effective, even if it were to be able to accurately identify every single person that walks into a store.

COUNCIL MEMBER HOLDEN: You're just against the technology that observes us.

NINA LOSHKAJIAN: Yes and, if it could actually make people safer, that's another discussion, but people who want to commit theft, they will put on a mask and I don't think we'll ever reach a point where that kind of obstacle can be overcome.

COUNCIL MEMBER HOLDEN: Let's just talk about cameras, because if I may, Chair, just one more, because Albert and I had some discussions in the past on this.

ALBERT FOX CAHN: A few, I always…

COUNCIL MEMBER HOLDEN: We had a few, but I respect your opinion. I do respect your advocacy. But we talked about speed cameras. We talked about red light cameras. You were kind of against that, too, at one point. You just said we shouldn't, that's

observing us. I have a camera system on my house because I need protection. If somebody comes into my yard or my driveway, I get an alert. That's a good thing, I think.

ALBERT FOX CAHN: And I think there's a world of difference between you operating that on your own property versus someone else operating…

COUNCIL MEMBER HOLDEN: Or a business operating to protect their property. That's not the same?

ALBERT FOX CAHN: I think there's a huge difference between something you open up to the world as a place where anyone can come and do business. That is a fundamentally different dynamic than a private home, and that's why, when we look at the laws governing public accommodations for nondiscrimination, for accessibility, it is a complete world apart, and I think with the camera systems we're talking about, the reality is they're not, these are systems that are ripe for abuse, as we've seen with Madison Square Garden, but also they can be used for any number of things. Think about a world where you're walking down the supermarket aisle

and every choice you make in the supermarket is being sold to advertisers as a way to better understand…

COUNCIL MEMBER HOLDEN: Well, some people feel Google does that now. I mean, you use your credit card, what happens? You buy something and you get so many other ads.

ALBERT FOX CAHN: I'm talking about the product you stop in front of, you think about, you decide, no, I don't want it. There are vendors that sell software out there to track just those behaviors.

COUNCIL MEMBER HOLDEN: But that's being done on everything, on your smartphone, it's done all the time. I mean, that's the kind of world, whether we like it or not, it's kind of evolved into that.

But one other question, in 1990, we had 122 burglaries. In 2024, we have 13,000. Because of technology, I feel, that's because of cameras. There are some good things. We talked about this at a previous hearing, that the camera that catches the serial killer that killed six people, and we caught them before they could strike again, what's wrong with surveillance in that regard on police matters?

ALBERT FOX CAHN: But Council Member, we have…

CHAIRPERSON GUTIÉRREZ: Council Member, can we wrap up? We have another set of questions.

ALBERT FOX CAHN: I would just say we have thousands and thousands of cities around the world which have deployed different types of technologies, and we can look at those as an experiment to see whether the use of cameras correlates with the reduction in crime, and the data is clear. It doesn't, and I would say that if it was as simple as that, with cameras just being the cure-all, we would see very different crime rates in a lot of American cities. We would see very different public safety scenarios around the world and, to me, I would say it's clear that there are very different factors that are pushing those trends.

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

CHAIRPERSON GUTIÉRREZ: Thank you, Council Member. I wanted to just wrap up, and I apologize, but I appreciate the discussion.

Would you agree, or would you suggest that New York State should take a comprehensive

approach to protecting personal data rather than addressing different types of data in the way that 18 other states have done?

ALBERT FOX CAHN: I think it would depend on the specifics of the law, but I'd say that New York needs to be much more aggressive in protecting its residents' data, and I think that a more comprehensive protection against biometric data collection in particular, and location data collection, would be an incredible milestone for the State.

CHAIRPERSON GUTIÉRREZ: Thank you. Regarding Intro. 539, Council Member Brannan's bill, would private action be sufficient for the bill to be effective or do you believe additional civil penalties are necessary?

ALBERT FOX CAHN: I'm always a belt and suspenders person when it comes to enforcement. If we can have robust agency action, and have a way for private actors to have their day in court, I think that has always been the most effective way to implement any of these safeguards.

CHAIRPERSON GUTIÉRREZ: Okay. Thank you all so much. Thank you for your patience and for your testimony.

We will call up the next panel. We have Fernando Brinn, Jake Parker, Robert Tappan, Adam Roberts, and Sharon Brown.

Thank you all for your patience and, once you're all settled, anyone can start.

Thank you. Yeah, just make sure your mics are on. Go for it.

ADAM ROBERTS: Thank you for holding this hearing today. I am Adam Roberts, Policy Director for the Community Housing Improvement Program, also known as CHIP. We represent New York's housing providers, including apartment building owners and managers. Our members operate rent-stabilized housing, which contains 1 million units of housing in New York City, making up 40 percent of its rental housing and the vast majority of its affordable housing. Intro. 425 is punitive to tenants who live in rent-stabilized housing as well as workers, including our members, who operate rent-stabilized housing. Rent-stabilized buildings generally do not have the financial resources to hire full-time doormen. Even so,

affordable housing must also be safe housing. This is particularly notable as rent-stabilized housing is in the midst of a major financial crisis. Across the city, net operating income is in a free fall, dropping as much as 20 percent in the Bronx year over year. The largest lender to rent-stabilized housing, Signature Bank, collapsed last year, and the now largest lender, New York Community Bank, has been saved by collapse by Trump's former Treasury Secretary, Steve Mnuchin, who has threatened to foreclose on our members en masse. The affordability rent-stabilized housing provides is entirely unsubsidized by the government. This means rent-stabilized housing does not have the operating revenue to cover basic expenses, let alone hire full-time doormen. Even if the financial crisis were to end, many buildings are too small to ever financially support full-time doormen. Therefore, rent-stabilized tenants and workers rely on more affordable security systems, such as virtual doormen and CCTV systems, to ensure their buildings are secure. In the future, they likely will use biometric identifiers, like fingers, voice, irises, and facial recognition. They, too, are more affordable than full-time doormen. This

bill is so broadly written that it bans any technology which can be used to establish individual identity. Every security system, from virtual doorman systems to fingerprint scanners, will be illegal. Technologies which establish individual identity have been used for decades to ensure safety in buildings which lack full-time doormen. We cannot imagine how tenants and workers will react to seeing CCTV and virtual doorman systems removed because of this bill. If the Council passes this bill, it will be depriving rent-stabilized tenants and workers the safety which wealthy New Yorkers enjoy in their homes. Again, thank you for holding this hearing today.

CHAIRPERSON GUTIÉRREZ: Thank you. We have questions, by the way, but we'll wait until the panel. Whoever wants to go next can go next.

FERNANDO BRINN: Thank you for allowing us to speak with you, Chairman. I want to address an issue that's been, as I'm sitting here, I'm looking at how the City looks at cybersecurity from the perspective of agencies. I'd like to take a minute and talk about cybersecurity from the perspective of the underserved community. So…

CHAIRPERSON GUTIÉRREZ: I'm sorry, can you just say your name for the record?

FERNANDO BRINN: Fernando Brinn.

CHAIRPERSON GUTIÉRREZ: Oh, Fernando.

FERNANDO BRINN: I am the CEO of the Brinn Group. We're a community-minded agency. We work with not-for-profits and community organizations. During the testimony that I heard, a couple of things came to mind. One was cyber insurance. Our community doesn't have cyber insurance. If they do, it's very high and very costly. Our not-for-profits that are receiving contracts from City agencies don't have a line budget for either cyber insurance. They don't have it for testing, penetration testing, for cyber and cloud security so what I'm saying is we need to look at how we can address this issue through our agencies because at the end of the day, Juanita Lopez, who gets up in the morning and goes to her health clinic or goes to her bank or goes to a community program for assistance, is giving her information to a system that's not protected so we need to ensure that those programs that are funded by the City Council and funded by the City are cyber secure, and I've put together a number of

organizations that I work with that are cyber security companies, and I would enjoy an opportunity to speak further on it. Thank you.

CHAIRPERSON GUTIÉRREZ: Thank you. Did you submit written testimony by the way?

FERNANDO BRINN: Yes, absolutely.

CHAIRPERSON GUTIÉRREZ: You did? Okay, all right.

FERNANDO BRINN: Yeah, within 72 hours, you'll have a whole written testimony from us.

CHAIRPERSON GUTIÉRREZ: Okay, perfect. Thank you, Fernando.

Okay, whoever wants to go next.

SHARON BROWN: My name is Sharon Brown.

CHAIRPERSON GUTIÉRREZ: Oh, Sharon, I'm sorry. Can you turn your mic on? Thank you.

SHARON BROWN: My name is Sharon Brown. How is everyone? Jesus loves you.

Okay, I think that it's very important that it is posted clearly that they have active bio cameras. It should not be a surprise to them the depth of how the camera can see them, their irises, the different things. If the camera can do certain things like that, it should be posted, or there's

going to be an issue of entrapment with these cameras. People viewing other people should have to alert them that they are viewing them specifically, and there should be a system where, if someone is being viewed on multiple cameras this way, that alerts come back to them if they're in some kind of system where they're being cyber-watched because that's a form of some kind of stalking where people are just cyber-watched. It becomes kind of criminal entrapment, different things like that. When the police go somewhere to see the video, if someone has been surveilling someone else, that's problematic that they're in a surveillance mode, that it lends against entrapment and also some kind of stalking, and the people who are going to be in the stores should have some kind of system where it goes back to, it can go back to the police, but they also need to still have regular cameras and things to back up because it's not a sure thing. I saw a person that was this tall, they were this short, they had this color hair, then they cut their hair or they take out the hair or something like that and it wasn't the person, so there should be more sure things there

like other backups. It shouldn't just be the cyber security.

CHAIRPERSON GUTIÉRREZ: Thank you, Sharon.

SHARON BROWN: Yes.

CHAIRPERSON GUTIÉRREZ: And whoever wants to go next.

JAKE PARKER: Hi, Chair Gutiérrez, Members of the Committee, I'm Jake Parker with the Security Industry Association representing more than 80 companies headquartered in New York and 1,500 nationwide. Our members provide safety and security products, among them the leading providers of biometric technologies including facial recognition software. Today these technologies contribute to the safety and security of our communities and bring value to our daily lives across many different types of applications. For example, uses by consumers for verification are rapidly expanding and the popularity is growing. From Mets fans using Entry Express for facial ticketing at Citi Field to speeding up TSA security lines at LaGuardia and JFK to faster debarkation at cruise ports in Manhattan and Brooklyn. Also, safety and security applications are helping stem the tide of retail theft which also

helps prevent food and pharmacy deserts in underserved communities by preserving access to grocery stores and other establishments facing pressure to close their doors. In all this, it's critical these technologies are used in a secure manner in ways that are lawful, ethical, and non-discriminatory. We're concerned with the two ordinances up for discussion on biometrics. These would simply outlaw most uses of biometric technologies despite the fact that they were already regulated under the City's existing Biometric Data Privacy and Tenant Data Privacy Laws. 217 would prevent the use by businesses and consumers regardless of the purpose and whether agreed to by the individual, robbing them of their choice to use more secure methods to verify their identity and also dictating limitations to New York businesses on how they can protect themselves and their properties. On that, it would reduce the ability of businesses to address organized retail crime which has risen 80 percent in recent years according to the City's recent report in conflict with the Mayor's initiatives that call for businesses to analyze and improve their security. It's important to remember

the human cost as well as the monetary cost. Retail crime is often violent crime. In the last two years more than 1,100 customers, employees and security personnel have been killed by criminals in retail settings across our country and the human cost is far beyond these victims as organized retail theft fuels drug smuggling, human trafficking and criminal enterprises. These technology tools are used daily across the city and the country to make stores safer. And I'll stop there.

CHAIRPERSON GUTIÉRREZ: Thank you, and we have the last panelist.

ROBERT TAPPAN: Yes. Hi. Committee Chair Gutiérrez and the New York City Council Members, thank you so much for inviting me. My name is Robert Tappan. I'm the Managing Director of the International Biometrics and Identity Association. We're an industry association whose member companies design and manufacture biometric products and technologies that span a wide array of use cases and different measurement types known as modalities which include fingerprint, iris and retina, speech recognition, DNA, and facial recognition among others. IBIA is chartered to advance the adoption and

responsible use of these technologies for managing human identity and to enhance security, privacy, access management, productivity and convenience for individuals, organizations, and governments. We do this through advocacy, engagement and education. I'm pleased to be back here today. My colleague, Jake, and I appeared before this Committee last year, and I'm very happy to be here again. Facial recognition technology has become an integral tool for ensuring public safety, preventing and deterring crime, protecting citizens and visitors, and enhancing security and convenience across many sectors. Prudent regulation is required, not prohibition. In the private sector, facial recognition enhances physical security for offices, residential buildings and facilities, not to mention access to secure method for accurate employee timekeeping. Retailers rely on it as part of their efforts to combat the rampant shoplifting plaguing this city and also around the country. This property crime threatens the viability of local stores and food access in underserved areas where they're forced to close due to excessive losses. We should be enabling businesses and

communities to address this public safety challenge, not tying their hands. Thank you for your time.

CHAIRPERSON GUTIÉRREZ: Thank you so much. I have a couple of questions.

Let me just gather my notes, excuse me. We'll go reverse order. Robert, you work with businesses particularly?

ROBERT TAPPAN: We have about two dozen member companies that provide a wide array of biometric equipment and technology.

CHAIRPERSON GUTIÉRREZ: Got it.

ROBERT TAPPAN: For government and private sector.

CHAIRPERSON GUTIÉRREZ: And private sector, okay. Do you have a sense of how many arrests were made after the facial recognition technology was installed in some of these private businesses?

ROBERT TAPPAN: Well, that's a hard statistic to come up with just a bold number because there are both governmental and law enforcement uses of it as well as private sector, and I don't think there's any comprehensive numbers of that magnitude just because I don't think it's measured that way.

CHAIRPERSON GUTIÉRREZ: But some of the small businesses would have, some of the businesses would have it, correct?

ROBERT TAPPAN: In certain jurisdictions, sure.

CHAIRPERSON GUTIÉRREZ: Okay.

ROBERT TAPPAN: I could provide that for you.

CHAIRPERSON GUTIÉRREZ: Okay.

ROBERT TAPPAN: Yeah.

CHAIRPERSON GUTIÉRREZ: In those instances of private businesses, do you know if the stores have signs informing people about the use of facial recognition technology?

ROBERT TAPPAN: Well, they should.

CHAIRPERSON GUTIÉRREZ: They're supposed to.

ROBERT TAPPAN: They should, yes.

CHAIRPERSON GUTIÉRREZ: But you don't know if every single business?

ROBERT TAPPAN: Well, again, this varies from jurisdiction to jurisdiction, which actually gets into a large.

CHAIRPERSON GUTIÉRREZ: I'm talking about just New York City though.

ROBERT TAPPAN: Well, New York City, again, there's laws in place or ordinances in place that stipulate that the warning should be there and available so that customers can see it. I am based in Washington, D.C. Do I know whether every establishment has signs? I don't have that answer for you.

CHAIRPERSON GUTIÉRREZ: Thank you. I just want to say hello to Council Member Marte's family. Hello. Como está?

Thank you. I apologize.

ROBERT TAPPAN: No worries.

CHAIRPERSON GUTIÉRREZ: A mom was in the building. Okay.

Fernando, you brought up a very good point about just equity in our communities and who has access to cybersecurity insurance. What are some of those instances where a small business, and I think sometimes we don't think of like a bodega necessarily having a cybersecurity compromise, what are some of those like small businesses or businesses that are having a lot of issues in communities of

color where they don't have access to cybersecurity software? What does that mean? What is the impact of that on a small business?

FERNANDO BRINN: Well, on a small business, a mom-and-pop store usually would not have internet capabilities. Where you're looking at a community agency that deals with mom-and-pop stores, deals with health centers, they would, and they would have to pay a cyber insurance fee every year. In addition to that though, they would also have to be able to prove that their cyber resilience, which is testing to make sure that their infrastructure is sound, which is done through a number of ways. If they're on the cloud, then it's done through WAF, CHOMP, which monitors and makes sure as if there's any intrusions that is dealt with immediately and reported back to the customer. In terms of pen testing, that's done in for-profit and non-for-profit community programs that want to ensure that their infrastructure is sound.

CHAIRPERSON GUTIÉRREZ: Thank you, and are you aware of businesses that potentially sell data from facial recognition system for marketing or other analytics outside of safety?

FERNANDO BRINN: No.

CHAIRPERSON GUTIÉRREZ: No, so it's primarily for?

FERNANDO BRINN: It's primarily for non-for-profits who engage and work with communities of color that gather information, help them through whatever issues they're having with the social service of the city, have contracts with the City so imagine there's a non-for-profit who has a contract, let's say, with the Department of Homeless Services and they're delivering services. Well, they have to maintain an infrastructure and, in that infrastructure, they have to ensure that that infrastructure is cyber resilient so there's pen testing, penetration testing. There's also looking at the dark web to make sure that that information isn't being sold to suspicious characters. That's a costly sum of money, and it's not a part of their operating budget through funding from City agencies so I think the issue here is that we're not allowing our non-for-profit providers the ability to be cyber resilient because it's not part of their funding so one thing we need to look at is how we can rectify that.

CHAIRPERSON GUTIÉRREZ: Thank you so much, Fernando.

My last question is for primarily Jake, Adam, and Robert. Same question. Curious if you, in both Robert and Jake instances, are you aware if businesses or private entities that you work with collect and share and even sell biometric data for other marketing or analytics or is it primarily for public safety? And Adam, curious on the private dwellings and residential dwellings, if there's signage obviously in the buildings and how long is this biometric information stored for?

ROBERT TAPPAN: Can I just jump in real quick from my vantage point? Our members do not buy and sell biometric information. Number one, biometric information is something that it can't be reverse engineered, and it's usually proprietary to each of the different technologies that these companies are developing so that's the beauty of this biometric information. It's unique to the individual, and it's also unique to the technology.

Second of all, I don't know if you are aware of this but, not too long ago, the State of New York and other jurisdictions all around the country,

State governments were selling driver's license information so I'm not saying that everybody is guilty of this, but information brokering is something that has been going on for years and years and years. Whether it's right is not up to me, but it's happening and it happens on the government side as well as the corporate or enterprise side. That's something also, there was a reason that that information was being sold by the State. It was very, very lucrative, and governments have to do what they have to do to meet their budgets and so do enterprises.

JAKE PARKER: Yeah, I'll just echo what Robert was saying. The way the biometric technology works, that information is useless outside of the system that created it, and so that's why there isn't a market for biometric data in that sense.

I wanted to go back to your other question though, too, regarding arrests. I think when you're looking at retail security and loss prevention programs, arrest is not the right measurement. I think it's definitely going to vary store to store and business to business, but it's the reduction in the overall incidents that they have, and so most

often this involves de-escalation, not a call to authorities, so repeat offenders entering stores are flagged for the goal of providing excellent customer service versus apprehending them, which typically results in fewer visits by these individuals. I've heard anecdotally one company reported they saw a 90 percent reduction at their locations after following a similar process to that.

Also, it's not just about theft. There's also public welfare and life safety uses that are appropriate. For example, one of our members told me that for their customers reported recovering over a dozen missing children after their customers were able to leverage the same technologies in response to Amber Alerts and something called Code Adam, which is a missing child safety system used in retail stores.

CHAIRPERSON GUTIÉRREZ: Thank you.

ADAM ROBERTS: Regarding apartment buildings, I mean, I think an important thing to emphasize about the bill as it’s currently written is it would ban much more than just, I think what we're talking about is biometric technology or facial recognition. It would ban essentially any video system so CCTV, virtual doorman, that would all be

made illegal and have to actually be removed, again, as the bill is currently written so, currently, I don't think most buildings have signage saying you're on camera or anything like that. I think it's just generally socially assumed that if you walk into an apartment building, there will be some sort of camera monitoring who's entering and exiting. That being said, I mean, if apartment buildings were to start using facial recognition, I'm sure there would be some signage put up. I mean, most of our members aren't, at this point, storing biometric data so I don't really have a good answer on that but, again, I would hope that the Council would establish some standards on how that is done.

JAKE PARKER: Can I add something to that?

CHAIRPERSON GUTIÉRREZ: Sure.

JAKE PARKER: Yeah, so some of our members do provide these types of systems that you're referring to, virtual doorman systems, so it’s important to point out that the current City Tenant Data Privacy Law requires the uses of electronic systems be voluntary and so, if it were to use biometric functionality, which is available, for those enrolled, they pre-enroll, they have automatic

access through the camera at the door. For those that are not enrolled, the system simply reverts back to a manual process so this could be connected to an operator who takes other steps to verify whether the person is a tenant or a guest or a delivery person, something like that.

SHARON BROWN: Can I say something?

CHAIRPERSON GUTIÉRREZ: Yeah, just turn your mic on.

SHARON BROWN: It's on. Just like they have a do not call list, I think with the information that has already been gathered, if the bill is passed and they outlaw these things, there should be a do not sell that information that's already collected or in the future, whatever they decide, it should be a list out there to say, don't put any of this information out there further, I'm not interested in having my information sold, like don't pass on my number, don't pass on my information. Maybe there should be some kind of registry or something and it can have some criteria.

CHAIRPERSON GUTIÉRREZ: In any of your line of work or for your clients, do any of you have any concerns about identity deepfakes or AI-

influenced images in the way that businesses, partners, non-profits are capturing biometric information?

JAKE PARKER: Yeah, sure. It was mentioned earlier that a concern about using biometric data to impersonate your identity. The way biometric information is created and used, that is just not possible. There are concerns about using deepfakes perhaps to impersonate someone who's doing some kind of authentication, using their face, and that's something that the industry is definitely on top of. There's a technology called liveness detection and authenticity detection in video that's often a layer onto those systems.

SHARON BROWN: Can I say something? Is the system smart enough to detect, what if I said, hey, I'm going to look like you and I got eye color, the eye…

CHAIRPERSON GUTIÉRREZ: Contacts?

SHARON BROWN: Contacts. I don't wear them, sorry. The contacts, I've got a hair like yours and I put on the makeup and I try to beat the system. Would it be able to detect that? People are getting plastic surgery to look like other people and so many

different things so is that system smart enough to detect that there's a fake, actual human AI that went to a plastic surgeon to look like this person next to them so could it pick that up in that system? Is it smart?

CHAIRPERSON GUTIÉRREZ: That's a good question.

SHARON BROWN: Well, I deal with technology myself. I let the other people build it, but I deal with the technology so could someone beat that system by just putting on contacts and hair and the same kind of dress that someone wears and put makeup, contour their face with makeup? Could they beat it and put on the same color eyes, change the shape, look with tape?

CHAIRPERSON GUTIÉRREZ: I'm not sure.

SHARON BROWN: With tape?

CHAIRPERSON GUTIÉRREZ: I hear you. I hear what you're saying.

SHARON BROWN: Okay, let's just say I want to look Asian today.

CHAIRPERSON GUTIÉRREZ: No, I got it, I got it, ma'am. I got it, I got the example. No, I got you. I'm not sure. I don't know if I'm equipped to

answer that question. I don't know if anyone here wants to answer it.

ROBERT TAPPAN: I would just simply say the answer to your question is no. The technology is such that it can detect all of the different types of fakery that goes on when people try to disrupt the system.

SHARON BROWN: And even surgery?

ROBERT TAPPAN: Even surgery. The beauty of the human body is that we are all unique. We all have a set of bones and genes and makeup and irises and retinas that are all unique. You can't fool those sorts of things.

CHAIRPERSON GUTIÉRREZ: I'm so sorry. I just have to get them to answer their questions because we do have other panelists. I apologize.

Does anyone else want to weigh in on my original question about deep fakes or concern about that?

ROBERT TAPPAN: If I could?

CHAIRPERSON GUTIÉRREZ: Yeah,

ROBERT TAPPAN: I'm sorry. So to answer to that question is, is it ever going to be 100 percent accurate? No. And that's what every hacker strives

for and that's what every company strives for. By putting limits on biometrics, you are actually hindering the progress and innovation that legitimate corporate businesses are doing to make it more accurate, to go beyond the deep fake, to be able to tell what is accurate and what isn't, and so it's a never-ending battle. It's like the Cold War, but now it's in biometrics so overcoming those things is a constant battle that needs to be won by the side that is trying to do something that's right as opposed to deceive.

SHARON BROWN: And just one last thing.

CHAIRPERSON GUTIÉRREZ: Yes.

SHARON BROWN: Okay, so he said you can't beat the system because we have different bones. Well, I know specifically people, if they have a bump on their nose, they shave it so they're shaving bones and doing different things in the surgeries so could something like that beat the system? So say for instance, my nose is like this today. I can go into surgery and get it shaved down and get it contoured, make it smaller. I can get my bone in my chin shaved down to be pointier. Could that beat the system and look like, appear like someone else? Would you be

able to pick that up? That's something that you really need to look into because people are going that in depth in surgery. The nose is the oldest one. They shave down the bone in the nose. Thank you.

CHAIRPERSON GUTIÉRREZ: Thank you. We're going to have a Council Member Hanif ask questions and then Council Member Holden.

COUNCIL MEMBER HANIF: Thank you. I just wanted to point out that Intro. 217 isn't a full blanket ban on biometric surveillance, and there are exceptions, especially when it comes to pay by palm at grocery stores or verification at the airport for travel documents so I just want to be clear that Intro. 217 is not saying no, and we recognize that there are some industries that require biometric surveillance for its functions so I just wanted to point that out.

I want to ask, what is your response to the FTC's finding about Rite Aid and what happened there? I mean, I'm sure that created a bit of a controversy. That case specifically running from 2012, the investigation is from 2012 to 2020 involving Rite Aid, and the vast egregious misuse of

this technology is very obvious and very clear. How do you respond to that?

JAKE PARKER: Well, I'm glad you asked that question so first of all, we support FTC's calls for having reasonable safeguards and the elements they lay out in that particular case. However, keep in mind, this program started in 2012, which was ancient times in respect to this technology. They were using a very outdated technology, first of all, but it was also highly unusual in the way it was implemented, and we believe it's an outlier that's not representative of how these programs are implemented today, and also keep in mind that this stemmed from a process from a 2010 order having to do with other types of customer data that they're supposed to be protecting and this decision came out as a result of that. But, in any case, the elements that the FTC said were needed to address the shortfalls are reflective of many safeguards that are already integrated in today's software and use policies and recommended practices and so we fully support those. I think going back to the earlier point about how effective is this, dozens of the top 100 retailers in the United States, in addition to

the small businesses that we're talking about, use this technology on a daily basis and are having success with it.

COUNCIL MEMBER HANIF: Then the businesses that you represent, are they primarily New York City based?

JAKE PARKER: No, so our members are the providers of the technology that the retailers use. Some of them are.

COUNCIL MEMBER HANIF: The providers are providing this technology to New York City commercial businesses.

ROBERT TAPPAN: As well as the TSA, DHS.

COUNCIL MEMBER HANIF: Right, right.

ROBERT TAPPAN: Yes.

COUNCIL MEMBER HANIF: But I'm mostly interested in the businesses in New York City. Is that true for both of your corporations?

ROBERT TAPPAN: I'm sure some of our members provide biometric technology…

COUNCIL MEMBER HANIF: Yeah, how many of your members that are New York City based?

ROBERT TAPPAN: I don't know if they're, I'd have to get back to you on that. I don't know.

COUNCIL MEMBER HANIF: Oh, you don't have that answer. And what about for you?

JAKE PARKER: Yeah, we have like 1,500 members.

COUNCIL MEMBER HANIF: That are New York City? 1,500 technology…

JAKE PARKER: We have several dozen that are headquartered in New York City.

COUNCIL MEMBER HANIF: Okay, I'd like to get that response as soon as possible.

I also just wanted to understand, and this is my final question because I know we've got another hearing here. Given your point about how the technology that was used in Rite Aid's instance is like from a different era and like there's been parameters that have like made this technology more efficient, what are the safeguards that the companies are using to prevent misuses like in the instance of Rite Aid, and what has been done to test for efficacy and accuracy?

ROBERT TAPPAN: Well, the National Institute of Science and Technology, NIST, is the gold standard for the measurement of the accuracy of biometrics writ large, especially when it comes to

facial recognition so it's an (INAUDIBLE) subset of the U.S. government.

COUNCIL MEMBER HANIF: So there's like a laboratory. NIST is a laboratory where you're testing…

ROBERT TAPPAN: That is correct, and companies are constantly testing the efficacy of their algorithms, of their technologies, and the efficacy by race, by sex, by gender, etc. in order to make it as accurate as possible.

One point of clarification, Councilwoman, you had talked about biometric surveillance and that's kind of, I'm sure that's one of those phrases that it comes very easy, it trills off the tongue, but biometrics is about verification and authentication. When you go to the airport, you submit your driver's license, you get your picture taken at the kiosk, it verifies that the credential that you presented is indeed the face that's on there is the same face that's in front of the kiosk camera and also verifies that the credential itself is valid.

COUNCIL MEMBER HANIF: Right.

ROBERT TAPPAN: But it's not surveillance. It's not following you around.

COUNCIL MEMBER HANIF: Intro. 217 isn’t that. But Intro. 217 isn't a ban on that because TSA's core function requires that authentication.

ROBERT TAPPAN: But I'm saying just the use of this type of technology is not surveillance. It is about authentication. If you're trying to catch the shoplifter who comes into a bodega day-in and week-in and week-out and keeps on stealing the same things and there's facial recognition in there, it is to authenticate that the person is a repeat offender, not to know where he goes or she goes after they steal something. It's not geolocated like that. It's not about following people around or knowing where they are. There are other technologies that do do that, but that's another part of your hearing, but biometric authentication and verification is about the person who says they are is who they are.

COUNCIL MEMBER HANIF: Right, what Intro. 217's goal is is that there are many, many instances of misuse of this technology that is surveilling certain individuals and predominantly black and brown people and primarily women of color so that's what

it's getting at. That's what it's getting at, and Rite Aid is a clear example if you want to talk about a recent example.

SHARON BROWN: Can I say something?

CHAIRPERSON GUTIÉRREZ: You have to hurry up. We have another Council Member who has questions. Is it a question or a response?

SHARON BROWN: It's a response.

CHAIRPERSON GUTIÉRREZ: Okay.

SHARON BROWN: Okay, so I think it would be a problem with authenticating someone. Say for instance, the two of you have your hair pulled back so if you take a picture of someone on an ID, you can see the shape of their face based on having your hair pulled back so if someone has their hair pulled forward and they have a picture, someone else comes in with the same kind of hairstyle, they could authenticate that it's them, quote unquote, but it's not really them because they can't see their features to know if this is actually the person so the accuracy is not there for them to use this solely to catch someone. It can be in addition to something else. It can't be solely because, say she has her hair pulled over and one is back and if you take a

picture of her on her ID, you don't know she could have a piece of her ear missing or some birthmark or something like that that you don't know about, and will the authentication process pick that up? Will it pick up certain things that you can't see?

CHAIRPERSON GUTIÉRREZ: That's another question and it's a similar question.

SHARON BROWN: It's rhetorical. I'm not really asking the question.

CHAIRPERSON GUTIÉRREZ: No, I understand and I'm so sorry. We just have to move on, but your comments and your questions are recorded.

JAKE PARKER: Was the Council Member's question also directed to me? I didn't know if you…

CHAIRPERSON GUTIÉRREZ: Say that again?

JAKE PARKER: Was the Council Member's question also directed at me, the previous one?

CHAIRPERSON GUTIÉRREZ: That was 90 seconds ago.

COUNCIL MEMBER HANIF: Sorry, I have already forgotten what it was.

CHAIRPERSON GUTIÉRREZ: It's okay. Well, we do have to move on because we do have another

hearing so I'm going to pass it to Council Member Holden.

COUNCIL MEMBER HOLDEN: Well, Mr. Parker, I'm going to give you a chance to opine on this because what we just heard is that the facial recognition software is biased and, maybe that was the case, like you said, in 2012. In your testimony here, a written testimony, you state numbers. Do you want to repeat what you wrote here?

JAKE PARKER: Yes.

COUNCIL MEMBER HOLDEN: Because I think we need to hear this because there's a shoplifting epidemic in New York City, and the timing of this bill, 217, is curious. I just find it strange, but give us the updated 2024 accuracy of facial recognition.

JAKE PARKER: With that type of application, there's two things that are key, is the technology performance, but also the governance structure that goes around it. On the technology performance, today's facial recognition technology, leading technologies as measured by the government's program under NIST, are all over 99 percent accurate across the board and, across 70 different demographic

factors they measure, it's 97.5 percent accurate so that's a far cry from where we were just even…

COUNCIL MEMBER HOLDEN: So we keep hearing how it's not accurate, but you're saying, and you're in the industry, it's accurate.

JAKE PARKER: Unfortunately, there's a lot of old information out there that keeps circulating.

COUNCIL MEMBER HOLDEN: It keeps resurfacing and, in my research, I found that out, that it's very accurate, but what's the alternative? If 217 did get through, what's the alternative? It's really somebody saying, this person looks like the guy I just saw, take this. How accurate is that?

JAKE PARKER: Exactly, without the technology, you're back to a manual process where you've got flipbooks of photos, posting photos on the break room wall in the store or something like that. People, humans, security guards, trying to do this kind of recognition at scale was very difficult, and I think that actually is one of the issues, I think, with the language. It was mentioned that the language is intended to preserve voluntary uses of the technology. Well, the problem is, the way it's written, it says that it's only an exception to the

ban if it must be used to perform that process, if the technology is required and, in almost every instance, it's not required, it's a way to improve a pre-existing process. Stores had loss prevention programs in place before, now they can do it better.

COUNCIL MEMBER HOLDEN: Thank you so much for that.

CHAIRPERSON GUTIÉRREZ: Thanks, Council Member.

Okay, my last question for this panel. Is there a way or a process for a person to delete their image in the same way that I had asked the panel previously, and I think I read a little bit in your testimony quickly.

JAKE PARKER: Yeah, so that's part of the government's piece, I mentioned. In addition to having good technology, you have the right policies and procedures in place so certainly, best practice here, and as far as I know, being carried out is providing clear notice at customer entrances, which is already the law in New York City but, also, people do have to be given a means to contest their enrollment in a kind of program. We certainly believe that, and then there needs to be a quick response to

any complaints raised, and there's other things that are key to a successful governance program, making sure that there's strict conditions that govern the enrollment to begin with. Only authorized people have access to that information, and then also that there's adequate training of the staff that this alert goes to as far as what to do in different situations. Those are all things that failed in the example that was mentioned before, but I believe are best practices out there today.

CHAIRPERSON GUTIÉRREZ: Thank you, and then the last question is, Intro. 217, besides the limitation on identification by facial recognition technology, requires a number of requirements, such as cybersecurity safeguards, a written retention policy, and written consent in advance of any biometric collection. Do you agree that all of those requirements are reasonable and necessary? Could be a quick yes or no.

JAKE PARKER: To the gentleman's point over here earlier, I think that is going to be an enormous burden on New York businesses because of how broadly that new definition would be scoped, what kinds of information would have to be subject to

policies on retention, destruction, security, control, monitoring, etc., because it has to do with any data of any person, which is not just employees or consumers, but even people located outside the city potentially.

CHAIRPERSON GUTIÉRREZ: Great.

ROBERT TAPPAN: I would also say, if you're talking about places of business, the people who are not going to opt in or do that could, are most likely shoplifters themselves. I mean the problem is that if there's a general policy that everybody has to adhere to, then that's fine. That's agreeable and reasonable but, in every situation there, you can't make it onerous on small businesses to have the same sort of policy that a department store has.

CHAIRPERSON GUTIÉRREZ: Okay. Thank you all so much. Thank you for your patience and your participation.

I'd like to call up our last panel, which is on Zoom, Daniel Schwarz and Hally Thornton.

SERGEANT-AT-ARMS: Starting time.

CHAIRPERSON GUTIÉRREZ: I'll call on Hally Thornton first.

HALLY THORNTON: Hello. Thank you so much for allowing me to testify virtually today. Good afternoon. My name is Hally Thornton, and I've been a resident of New York City for 14 years, and I'm testifying today on behalf of Fight for the Future in support of banning facial recognition in public places and residential buildings. Fight for the Future is a digital rights organization with over 2.5 million members nationwide, including over 85,000 in New York City. I'm a staff member at Fight focused on administrative and campaign support. Our group is strongly opposed to the use of technologies that collect people's biometric data and store that data en masse in the cloud. This includes the facial recognition tools used in places of public accommodation and residential buildings. Once companies collect this data, we have virtually no way of knowing how they'll use it. They can sell it to data brokers or share it with abusive law enforcement agencies. Facial recognition technology enables mass monitoring and tracking at a previously impossible scale and, each time biometric data is shared or leaked, it brings us one step closer to a world in which everyone is identified wherever they go and

privacy no longer exists. Databases of biometric information, unchangeable bodily data, have also already been hacked, posing unprecedented risks to people's privacy and safety. Industry groups will claim that the data they're collecting isn't useful to hackers or anyone else, but that's not the case. If companies create systems for identifying people who are otherwise anonymous using facial recognition, then law enforcement, hackers, and others can abuse and/or recreate those systems. As the New York Department of Education concluded after studying the use of this tech in schools, the harms of facial recognition far outweigh any possible benefits. Facial recognition has been banned in New York schools and we urge the Council to ban it in places of public accommodation and residential buildings. Thank you.

CHAIRPERSON GUTIÉRREZ: Thank you, Hally. Our last panelist is Daniel Schwarz.

SERGEANT-AT-ARMS: Starting time.

DANIEL SCHWARZ: My name is Daniel Schwarz, 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. Biometric surveillance tools enable and amplify the invasive tracking of who we are, where we go, and who we meet. They're also highly flawed and racially biased, and I'm happy to go more in depth on that after my oral testimony. The widespread use of these technologies presents a clear danger to all New Yorkers' civil liberties and threatens to erode our fundamental rights to privacy, protest, and equal treatment under the law. The Council must ensure New Yorkers are not surveilled, targeted, discriminated against, and criminalized on the basis of invasive, flawed, and biased technology. To this end, we call for prohibitions on biometric surveillance in areas of severe and power imbalance, including its use by law enforcement or other government agencies, in housing, and in other areas where our fundamental rights are at stake or where informed consent cannot be given. The NYCLU supports Intro. 217 to prohibit places of public accommodations from using biometric surveillance and require written consent for any collection of biometric data. The face recognition deployment by MSG to target staff from law firms in litigation with MSG points to Orwellian use cases

where it will be impossible to move and associate freely, and the technology's racial as well as gender bias risks disproportionately impacting women and people of color, such as in the misidentification of a black teenager that barred her from entering an ice skating rink or in that of a woman in the UK just recently who was misidentified as a shoplifter and subsequently bag-searched, asked to leave the store, and banned from all stores using the same vendor. Raising related harms, the Federal Trade Commission, as we heard, successfully brought charges against a large retailer, Rite Aid, which is now banned from using facial recognition after similarly falsely identifying consumers as shoplifters. For these reasons, we support banning biometric surveillance in places of public accommodation. To ensure that the legislation fully meets its goals, we make detailed recommendations in our written testimony. Intro. 425 would prohibit landlords from using biometric recognition technology.

SERGEANT-AT-ARMS: Thank you. Your time has expired.

CHAIRPERSON GUTIÉRREZ: Oh, we have your testimony, Daniel. Do you want to wrap up?

DANIEL SCHWARZ: Yeah. Just in conclusion, I say 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 they exercise their free speech rights. The NYCLU supports Intro. 217 and 425, and we urge for this with passage. For similar reasons, we also support Intro. 539 to prohibit the sharing of location data with third parties. Thank you.

CHAIRPERSON GUTIÉRREZ: Thank you so much, and we do have your full testimony. Thank you for submitting that.

If we have inadvertently missed anyone who has registered to testify today and has yet to have been called, please use the Zoom hand function and you will be called in the order that your hand has been raised.

Okay, no one.

Thank you, everyone, for your testimonies today. The hearing is adjourned. [GAVEL] Adios. Thank you, everyone.

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 July 6, 2024