CITY COUNCIL
CITY OF NEW YORK

------------------------ X

TRANSCRIPT OF THE MINUTES

Of the

COMMITTEE ON TECHNOLOGY

------------------------ X

March 2, 2026
Start: 10:12 a.m.
Recess: 1:14 p.m.

HELD AT: 250 BROADWAY - 8TH FLOOR - HEARING ROOM 2

BEFORE: Carmen N. De La Rosa, Chairperson

COUNCIL MEMBERS:
Shahana Hanif
Julie Won

OTHER COUNCIL MEMBERS ATTENDING:
Pierina Ana Sanchez
Jumaane Williams, Public Advocate

APPEARANCES

Alex Foard, Assistant Commissioner of Research and Collaboration in the New York City Office of Technology and Innovation

Lucy Joffe, Deputy Commissioner for Policy and Strategy at New York City Housing Preservation and Development

Laura Moraff, Staff Attorney at the Legal Aid Society's Digital Forensics Unit

Nina Lashkajian, Technology and Racial Justice Collaborative Fellow at the Center on Race, Inequality, and the Law at NYU Law

Talia Kamran, Staff Attorney with the Seizure and Surveillance Defense Project at Brooklyn Defenders

Jake Parker, Security Industry Association

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

Shruthi Velidi, Democrat Socialist of America's Tech Action Working Group

Medha Raman, New York Civil Liberties Union

Cynthia Conti-Cook, Director of Research and Policy at the Collaborative Research Center for Resilience

Sergio De La Peña, Legal Director of New York County Defender Services

APPEARANCES (continued)

Corinne Worthington, Advocacy and Community Engagement Manager at the Surveillance Technology Oversight Project

Michele Anne Blondmonville, self

Christopher Leon Johnson, self

SERGEANT-AT-ARMS: Quiet down, please. Good morning, and welcome to today's New York City Council hearing for the Committee on Technology.

If you would like to testify, you must fill out a witness slip with one of the Sergeant-at-Arms, even if you signed up online already.

At this time, please silence all electronic devices, please silence all electronic devices and no one may approach at any time.

Chair, we are ready to begin.

CHAIRPERSON DE LA ROSA: Good morning, and welcome to our first hearing. I'm Council Member Carmen De La Rosa, Chair of the Committee on Technology. Thank you for joining us for today's oversight hearing on facial recognition technology and the collection of biometric data. We will hear two bills, Proposed Intro. 213-A sponsored by Council Member Hanif in relation to prohibiting places or providers of public accommodations from using biometric recognition technology and protecting any biometric identifier information collected and Intro. 428 sponsored by Council Member Pierina Sanchez in relation to limiting the use of facial recognition technology in residential buildings.

This is my first hearing as a Chair of the Committee on Technology, and I'm very excited to start this session with this important topic. Facial recognition technology was introduced years ago and, since then, it has advanced rapidly in both accuracy and accessibility. It is without question an impressive and innovative tool. Today, it allows individuals to unlock their phones instantly, secure access to devices and sensitive files, and enhance certain security systems. Used responsibly and with appropriate safeguards, facial recognition technology offers convenience and efficiency. However, like many powerful technologies, its impact depends entirely on who is using it and how it is used. Some argue that facial recognition is necessary for public safety. Cameras are now present on many street corners, in public accommodations, transportation systems, retail stores, and even residential buildings. Yet the widespread presence of cameras and facial recognition systems has not by itself eliminated crime. Retailers may argue that facial recognition helps combat shoplifting and organized retail theft. However, long-term theft statistics in New York City from 2006 to 2024 show that overall trends have generally increased, with temporary declines during the 2020 lockdown and slight decreases in 2023. Technology alone has not proven to be the comprehensive solution. Additionally, no technology is perfect. Facial recognition systems still misidentify individuals. According to testing by the National Institute of Standards and Technology, error rates can be below one percent when analyzing high-quality controlled images such as mug shots. However, when images are less clear, such as those captured by surveillance cameras in real-world conditions, the error rate can increase significantly, in some cases approaching 20 percent.

Even if accuracy could be perfectly improved, serious concerns still remain. What happens when a person is wrongfully flagged as a criminal because he or she is standing near someone else, resembles another individual, or were mistakenly included in a database? What recourse does that person have to correct inaccurate information? Is there a transparent process for review and removal? Consider another scenario. A person who once committed a minor offense out of necessity or under duress or by accident, should that individual be permanently barred from entering grocery stores or denied housing because of biometric data stored in a private system? Without clear standards and due process protections, private entities may impose penalties without transparency or an opportunity for appeal. We have already seen this technology used beyond traditional security context. Madison Square Garden made headlines for using facial recognition technology to deny entry to certain attorneys involved in litigation against the company. That raises an important question. Where are the boundaries? Could this technology be used to exclude individuals based on profession? Could it be misused to discriminate based on political views, skin tones, backgrounds, or other characteristics? The risks become even more significant when facial recognition is combined with artificial intelligence and other data sets. Could facial recognition data be linked to financial records, credit scores, tax information, purchasing history, or family status? Could individuals be excluded based on income level? Could different services be provided based on data that has been aggregated about a cost a customer? These concerns are no longer theoretical.

And one more thing, unlike a password or a credit card, a face cannot be easily changed. Once biometric data is captured, the risk could be permanent. Unfortunately, the law often lags behind technological advances. This is why thoughtful action is necessary now. Innovation should not come at the expense of fundamental rights. Clear guardrails are essential. Transparency is how systems operate meaningful consent, limits on data retention and sharing, strong anti-discrimination protections, independent oversight, and accessible mechanisms to correct errors.

Facial recognition technology is not inherently good or bad. It is a powerful tool. But its impact depends not only on how it's designed, but also on how it is used and for what purpose. Because of its power, it demands careful governance and clear boundaries. Our responsibility is to ensure that as technology evolves, it does so in a way that protects privacy, prevents discrimination, safeguards due process, and maintains public trust. The goal is not to slow innovation. The goal is to ensure that innovation serves people without compromising their rights.

Today, I want honest answers from OTI, from businesses and real estate owners, and from residents themselves about the real benefits and dangers of technology.

Finally, I'd like to thank technology Committee Staff, Attorney Irene Byhovsky, we're gonna get that, we're gonna get that, Irene, don't worry, and Policy Analyst Erik Brown, my Chief-of-Staff James Burke, and Fray Familia for their tremendous work on putting these hearings together. I also want to recognize Committee Members, Council Members Hanif and Council Member Sanchez, who are here, and I'll now turn it to Council Member Hanif for her statement on the bill.

COUNCIL MEMBER HANIF: Thank you, Chair De La Rosa, for holding today's important hearing and for including my bill, Intro. 213, on today's agenda. I'm proud that 14 Members of the Council currently sponsor this bill.

Intro. 213 would prohibit businesses and other places of public accommodation from using facial recognition and other forms of biometric surveillance to verify or identify a customer. This is 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 they walk, collected, used, or sold for targeted advertising or other purposes. This hearing comes at an important time. Earlier this year, New Yorkers learned that Wegmans has begun collecting biometric data from customers entering its supermarkets. That means that shoppers may have their facial features, eye scans, or voice data captured without a clear understanding of how that information is stored, used, or shared. What happens if that data is breached? Many of us know the feeling of discovering our credit card information has been stolen. It's invasive and frightening. But you can cancel a credit card and get a new one. You cannot cancel your face. You cannot replace your iris. You cannot change your gait. Biometric data is permanent. When it is compromised, the harm is lasting. That's why this issue demands urgent attention.

Intro. 213 is a critical measure to combat wrongful discrimination. Facial recognition tools have repeatedly been shown to produce significantly higher inaccuracy rates for people of color and women. Those inaccuracies are not abstract. They have resulted in real people being falsely accused of wrongdoing and denied access to public spaces. The Federal Trade Commission found that Rite Aid used facial recognition technology in a way that falsely and disproportionately identified thousands of people of color and women as likely shoplifters, including in New York City stores. The FTC described what followed, "acting on false positive facial recognition matches, employees followed customers around its stores, searched them, ordered them to leave, call the police to confront or remove customers, consumers, and publicly accused them sometimes in front of friends or family of shoplifting or other wrongdoing." In one case, an 11-year-old girl was wrongly stopped and searched because of a false match. I urge everyone here to imagine how dehumanizing that experience would be. It's reported that Madison Square Garden Entertainment used facial recognition technology to identify individuals and deny certain people entry based on their employer. That is a deeply troubling use of surveillance technology.

Discrimination and harm caused by biometric surveillance is not a paranoid hypothetical and not a one-off incident. It is happening now. While Rite Aid is prohibited from using biometric surveillance for five years, we shouldn't have to rely on federal investigations and lawsuits to prevent other businesses from repeating the same harm against New Yorkers. I also want to be clear this bill takes a measured approach. It does not ban all uses of biometric technology. Customers would still be able to opt in to technologies like pay by palm at checkout or biometric identity verification at airports. Businesses that genuinely require biometric tools to carry out core functions, such as a custom running shoe store that uses gait analysis, would be permitted to do so. This legislation advances basic consumer protections, not ideological absolutism.

And this bill does not affect standard security tools like video monitoring. I share concerns about retail theft and repeat offenders. And I support funding for infrastructure upgrades that help small businesses. But as a Rite Aid case demonstrates, biometric surveillance is not an effective solution. And in many cases, it makes 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 know firsthand the consequences of allowing fear to justify excessive and biased surveillance.

I want to thank the Ban the Scan Coalition, who rallied with us earlier today and are here to testify in support of Intro. 213. Thank you, Chair De La Rosa.

CHAIRPERSON DE LA ROSA: Thank you, Council Member Hanif.

We'll now hear from Council Member Pierina Sanchez on her bill.

COUNCIL MEMBER SANCHEZ: Thank you, Chair, and good morning, everyone.

When you come home at night, your building should be a place of safety, not surveillance. I reintroduced Intro. 428 because biometric recognition technology systems don't just unlock doors. They can collect and can store deeply personal information, your face, your gait, your movement patterns, and this information can track who you are, where you go, and who you meet. We know these technologies are still flawed and racially biased, as my Colleagues have highlighted. Study after study shows that they misidentify Black and Brown people at disproportionately higher rates. Housing is an area of profound power imbalance, and your landlord in particular should not have the automatic ability to build a biometric database of you as a tenant and your guests.

Intro. 428 is simple. It expands upon Local Law 63 of 2021, which placed tenant protections with respect to property owners that utilize smart access or keyless systems. Intro. 428 limits what smart access systems can collect and prohibits biometric recognition technology in multiple dwellings without explicit consent. We care about buildings and their security, of course, just not at the cost of tenant privacy and civil liberties. I also want to thank the Ban the Scan Coalition for your collaboration on this bill before I was a sponsor, because we agree that New Yorkers deserve their privacy. Thank you so much.

CHAIRPERSON DE LA ROSA: Thank you so much, Council Member Sanchez.

We are expecting the Public Advocate soon, but we're going to go ahead and hear testimony from OTI and HPD, and we also have some written testimony from DCWP covering their positions on the bill, so I want to welcome Alex Foard, the Executive Director of Research and Collaboration under OTI, and Lucy Joffe of HPD.

COMMITTEE COUNSEL BYHOVSKY: Thank you, Chair, and before we begin with your testimony, I kindly ask you to raise your right hands.

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

ASSISTANT COMMISSIONER FOARD: I do.

DEPUTY COMMISSIONER JOFFE: Yes.

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

ASSISTANT COMMISSIONER FOARD: Thank you. Good morning, Chair De La Rosa and Members of the City Council's Committee on Technology. My name is Alex Foard. I'm the Assistant Commissioner of Research and Collaboration in the Office of Technology and Innovation, or OTI. Thank you for holding a hearing on this timely topic. I'm pleased to have the opportunity to discuss my team's area of expertise with the Committee as it relates to today's oversight topic.

For those not familiar with our work, OTI's research and collaboration team leads the City's broad approach to artificial intelligence, or AI, policy and governance. We have built a comprehensive portfolio from the ground up and will continue to expand on it in this dynamically changing policy area. The cornerstone of our work is the AI Action Plan, a first-of-its-kind framework to support responsible AI use in City government. Since its publication in October 2023, we have released two public-facing progress reports documenting its implementation. This plan supports agencies as they evaluate AI tools and associated risks to determine whether these technologies can help them deliver better outcomes for New Yorkers. I'm pleased to report that we've nearly completed all the actions described in the plan.

Most recently, we updated policies on AI principles and definitions and generative AI preliminary use guidance in response to technological advances in the field of AI. Additionally, we created new guidance on how City agencies should engage the public in discussing the use of AI for digital service delivery and have developed new instructional material for all City personnel to establish basic literacy on AI, focusing not just on generative AI but addressing the City's definition of AI more broadly. We continue to carry out research and planning related to AI risk management, focusing on elements such as an AI risk taxonomy and a prototype risk assessment policy, risk review process, and risk monitoring process.

Another major responsibility of our team is leading agencies' compliance with Local Law 35. This law requires the disclosure of algorithmic tools that materially impact the rights, liberties, benefits, safety, or interests of the public. A subset of an algorithmic tool is one that collects biometric identifiers, i.e. facial recognition or fingerprints. In last year's report, three agencies reported the use of tools collecting biometric identifiers. This year's annual Local Law 35 report will be released later this month. I'm pleased to note that we have 100 percent participation from City agencies and will have a record number of algorithmic tools reported. This year marks the sixth cycle of compliance, and as we expand our guidance and offerings to municipal employees, we expect increased engagement from agencies in the future.

OTI is proud of our efforts to date to promote responsible use of AI tools in City government, and we will continue in the coming months to build on this strong foundation. Last year, we worked on a package of legislation with the Council, the GUARD Act, that requires the establishment of the Office of Algorithmic Accountability. This new office, which will be established by June, will undertake additional responsibilities that will expand on my team's work. These duties will include analyzing algorithmic tools submitted by agencies to determine whether there is a risk that the proposed tool could result in discriminatory decision making, conducting and publicly reporting on pre-deployment assessments, creating and maintaining a public-facing platform for submission of comments, establishing a protocol with the Department of Investigation for receiving complaints from the public, promulgating rules establishing basic compliance standards that all agencies must meet in developing, procuring, deploying, and using public impacting artificial intelligence, and expanding Local Law 35 reporting by publicly listing all artificial intelligence systems for which we have conducted a pre-deployment assessment.

We are also in the planning stages of implementing Local Law 25 of 2026, which requires us to conduct an AI workforce impact study with the Department of Citywide Administrative Services, DCAS. This study will examine the impacts of algorithmic tools and automated employment decision tools on employees and the administration of their municipal duties.

OTI views AI technologies not as an aid to replace city jobs, but as a tool to support City employees' efforts to serve New Yorkers. Our objective is to prepare City personnel, whether they serve in technical roles or not, to effectively and responsibly work with and on AI. To that end, the AI Action Plan and its initiatives dedicated to building AI knowledge and skills within City government will serve as our North Star.

As an update from the last hearing at which I appeared in June 2025, I wanted to share with the Chair that we are actively engaged with the Office of Labor Relations, OLR, on various efforts that my team leads. OLR is advising on the implementation of Local Law 25, has joined our AI Steering Committee, and has participated in our AI Speaker Series offered to City employees.

Thank you once again for the opportunity to testify today. I'm happy to take Council Members' questions.

DEPUTY COMMISSIONER JOFFE: Good morning, Chair De La Rosa and Members of the New York City Council Committee on Technology. My name is Lucy Joffe, and I'm the Deputy Commissioner for Policy and Strategy at the New York City Department of Housing, Preservation, and Development. Thank you for the opportunity to speak on Intro. 428, which would prohibit the use of biometric recognition technologies in residential buildings.

As an agency, we care deeply about the intersection of tenants' rights and data privacy. With the proliferation of biometric technologies in public and residential spaces, there are real fears about the potential sharing of, misuse of, or unauthorized access to identifying information. The collection and use of this data raises potential privacy concerns for all New Yorkers. However, immigrant communities, survivors of domestic violence, and formerly justice-involved individuals in particular, face heightened risks if sensitive data is improperly accessed or shared. These privacy concerns are compounded by questions about the reliability of these technologies and the equity implications that follow. We understand that there is growing evidence that certain biometric technologies can be inaccurate, as discussed so far already today, with documented disparities in performance across race, gender, age, and disability. Studies have shown that facial recognition systems in particular have higher error rates for women and people of color. In the housing context, inaccuracies are not a minor inconvenience. They could result in tenants being denied entry to their own homes or subjected to additional scrutiny. That risk raises serious equity and fairness concerns.

For these reasons, we support the goals of limiting the collection and use of sensitive identifying information in residential settings. We look forward to hearing more from the Council on how best we as a City can work collaboratively to address the concerns the bill seeks to address.

Thank you, and I welcome your questions.

CHAIRPERSON DE LA ROSA: Thank you so much.

I know that there's some testimony coming down from DCWP, but we're getting it printed, and it should be here shortly.

I'm going to ask one question, and then I'm going to turn it over to my Colleagues, because I know that there's a very important, also very important hearing across the street on universal child care.

So, I'm going to ask one question, which is a follow-up question that the Committee has asked before at our June 10, 2025, hearing and December 8, 2025, hearing, and we haven't received much information yet, so we're going to ask it again. Can you tell us what agencies collect biometric information, specifically fingerprints, iris scan, facial geometry, and voice print, and DNA?

ASSISTANT COMMISSIONER FOARD: Thanks for the question. So, the perspective that I can share on this, as I mentioned in my testimony, relates to the way that the City is using AI, so that's where our oversight is, and from that perspective, what we would be seeing is uses of biometric information in Local Law 35 reporting, which would be the algorithmic tools that have material public impact. The 2024 report had three tools total that were reported across City agencies that were leveraging biometric data somewhere in the decision-making process with those algorithmic tools. Other tools do use identifying information. That is a question that we ask of agencies as part of that reporting, but only three identified that it was biometric. I do want to indicate that agencies could be using biometric data in ways that aren't involved in algorithmic decision-making or AI or other uses, in which case we would not have visibility into that collection. That said, the collection of identifying information and biometric data would be covered under the Identifying Information Law. Biometric data are considered identifying information, so any use that agencies are using to collect or maintain those data would be governed by that law.

CHAIRPERSON DE LA ROSA: So, you mentioned that there's three. What are the three?

ASSISTANT COMMISSIONER FOARD: There is one tool from NYPD for facial recognition, one from

Department of Investigation for facial recognition, and then the Office of the Chief Medical Examiner for their DNA database.

CHAIRPERSON DE LA ROSA: Okay. I'm going to pause my line of questioning. I have more on that, so we'll hold that thought, but I want to give Council Member Sanchez and Hanif an opportunity before they have to head out. Go ahead.

COUNCIL MEMBER SANCHEZ: Thank you so much, Chair. A couple of competing hearings at the same time, but thank you for your testimony today, and I'm very happy to hear that you support the intent at HPD for Intro. 428.

So, I just wanted to understand how implementation of Local Law 63 of 2021 is going. You know, that law required property owners to provide tenants with a data retention and privacy policy with respect to their smart access systems, but also placed very important limits on what they could collect, how long they could retain it for. You know, it did a lot, and it also created a private right of action for anyone who believes their rights were violated with respect to that local law. So, in connection to 428, 428 would live in that part of the

Code, and so I'm curious as to whether or how HPD has been enforcing this local law and what you're thinking is at this time in terms of expanding that local law to include 428 and how we would enforce it.

DEPUTY COMMISSIONER JOFFE: Thank you for that question. HPD has been primarily charged under that law with education and ensuring that people understand their rights, which is incredibly important when we introduce new laws of this type. So, we see that as both important for us to ensure that tenants understand their rights and that owners understand their responsibilities. We use HPD's ABCs of Housing to ensure that we are providing both sets of groups with that information. It's also information that's available on our website, and so when we're out in the community, the ABCs of Housing is a primary tool for helping to make sure that folks understand those rights and responsibilities, also ways in which we collaborate with Members of the Council to make sure that we are sharing enough information appropriately. And, as you mentioned, this proposed law would mirror the enforcement structure there where we would continue to provide education, ensure that people are clear on their rights and responsibilities, and there's a very important private right of action.

COUNCIL MEMBER SANCHEZ: Thank you, and just a quick follow-up. So, is HPD doing no monitoring, receiving no complaints in connection to tenants who believe that their rights have been violated?

DEPUTY COMMISSIONER JOFFE: So, under Local Law 63, it did not charge HPD with monitoring or enforcement responsibilities is my understanding. So, we are carrying out our job as created under the law, and the private right of action is the supplement to the educational role that was created for HPD.

COUNCIL MEMBER SANCHEZ: Got it, and you're not aware of complaints? None of these come to the City, or you're not aware?

DEPUTY COMMISSIONER JOFFE: We're not aware of complaints or there being issues with implementation of the law.

COUNCIL MEMBER SANCHEZ: Thank you. And OTI, any comment? Are you aware of any complaints with respect to this local law?

ASSISTANT COMMISSIONER FOARD: No, and I would defer to HPD.

COUNCIL MEMBER SANCHEZ: All right. Thank you, Chair.

CHAIRPERSON DE LA ROSA: Thank you, and thank you, Council Member Hani, for staying a little longer, and thank you for being here, and I know there's a lot going on today.

I want to just go back to the frame of thought that we were talking about with the collection of biometric information. So, we know from reporting in the media, from lawsuits, that, for example, the Department of Correction does use voiceprint, and that DNA is collected by other agencies. So, can you walk us through the type of reporting that agencies right now are required to do in order to give OTI the information that you're giving to us today?

ASSISTANT COMMISSIONER FOARD: Yes. Great question. So, Local Law 35 has essentially three criteria for tools that need to be reported. First, the tool needs to be essentially driven by complex data analytics, so often that is AI. It doesn't have to be AI. Sometimes it's things like optimization algorithms and other sort of techniques to be able to do a more sophisticated data calculation. The second is that it has to be involved in some component of decision-making for the agency, and it has to be used at least once throughout the year. So, if an agency, for example, were experimenting with a tool to help them drive decision-making algorithmically, but they hadn't brought it into actual operation yet, it wouldn't need to be reported in that year. Or if they were using it, again, to sort of just inform some thinking, but not to actually drive a decision, it may not meet that criteria. And then the third criterion is that it has to have what is called a material impact, which essentially means a much more direct impact on somebody's access to benefits, rights, liberties, etc. And those three criteria are built into the definition of algorithmic tool in the law itself. OTI provides some additional guidance to agencies to help with sort of gray areas that can exist around those criteria, but essentially an agency needs to look at those three criteria against their systems and say which of these systems are meeting all three of those. If a system does not meet all three, it doesn't need to be reported under Local

Law 35. It doesn't mean there aren't other governance frameworks for that system. Again, the Identifying Information Law is a good example of something that applies whether something is an AI or algorithmic tool or not, but it would only be reported under Local Law 35 if it meets all three of those.

COUNCIL MEMBER SANCHEZ: And when there are cases like, for example, the lawsuits that NYCLU had a lawsuit, and in that lawsuit they discovered that DOCS was using facial recognition in all of its prisons. Does OTI then go back to DOCS and say, hey, there's this lawsuit, this information has been discovered, can you give us information on how you're using facial recognition?

ASSISTANT COMMISSIONER FOARD: We do work with agencies to better understand the requirements of the law generally, so we take our charge as the agency responsible for overseeing Local Law 35 to mean not just doing our own compliance and collecting everybody else's report, but aiding other agencies in doing their reports as well. We do an annual kickoff for Local Law 35 where we reintroduce the requirements. We have a liaison at every agency who's tapped to be able to be that agency's coordinator who works with us on that work. And then in the case that you're describing, if we sort of feel that there's something that we've heard of, whether through media or other places, we absolutely do have conversations with agencies to better understand the usage of that technology. Ultimately, the decision is always the agency's to understand if a given system in fact does meet those criteria. So, there could be instances where we talk to an agency and they make a determination, say, it doesn't seem to quite fit the entire set of criteria for reporting under Local Law 35, but that decision is ultimately the agency's to make.

CHAIRPERSON DE LA ROSA: I understand that that is the agency's decision, but I would think that OTI as, you know, the chief technology arm for the City, in the case where, for example, you know, we're talking about people that are incarcerated, right? There's not a population that is going to be able to defend itself from the use of facial recognition. If there is an instance, as the one pointed here through the NYCLU lawsuit, where it's clear that this technology is being implemented in a way, I would think that OTI would have more powers to be able to say, we need to see into this information, because it's not sufficient to just have the data and know that it's being used. You know, data, numbers, we can all sort of be like, oh, it doesn't fit that criteria, and figure out why it doesn't fit that criteria. I kind of want to understand sort of where are your enforcement mechanisms if it is determined that an agency is saying, well, that doesn't qualify, then what happens next?

ASSISTANT COMMISSIONER FOARD: Yeah. That's a great question. So, Local Law 35 itself doesn't have mechanism for OTI to enforce in that same sense of what you're describing. Agencies are the ones who are responsible for identifying the tools, reporting those to OTI. The GUARD Act that I mentioned will sort of enhance the requirements coming out of the new Office of Algorithmic Accountability to work with agencies on this sort of engagement to better understand their requirements under the law. That package of bills also included expanded reporting requirements for what we currently call Local Law 35. So, I do think that our existing engagement with agencies is already quite robust, and then we expect even more robust practices with them later this year.

CHAIRPERSON DE LA ROSA: Okay. Going back to Local Law 35, according to the report, DOI is using facial recognition technology. However, the vendor's name stated as not disclosable out-of-the-box products. The vendor provided ongoing technological assistance. Confidentiality agreements are in place with that vendor. Do you have any idea why that might be the case? Is it common practice to include an NDA as part of a contract?

ASSISTANT COMMISSIONER FOARD: I can't speak to the use of NDAs globally. That would be a bit outside of my purview. I think in the instance of Local Law 35 reporting, there is a line in the law that allows agencies to be able to withhold the sort of information that would put some of their work at jeopardy. I don't remember the exact language off the top of my head, but an agency can make that decision to say maybe some of this information would be problematic for us to have in this part of the report, but I would refer the specifics to DOI.

CHAIRPERSON DE LA ROSA: DOI. Okay. Let's see. I want to ask a question about the MTA.

According to The Record, a newspaper, the MTA is testing subway gates that use cameras powered by AI to collect people suspected of not paying fares. Do you know if these cameras use facial recognition? Is this something that would be reported to the agency?

ASSISTANT COMMISSIONER FOARD: I don't know that. It would not be something that would be reported. MTA does not have to report under Local Law 35.

CHAIRPERSON DE LA ROSA: Okay. I'm going to pass it over to Council Member Hanif, and then I'll come back for some other questions. Thank you.

COUNCIL MEMBER HANIF: All right. Thank you.

Okay. So, you mentioned that the NYPD Chief Medical Examiner's Office and DOI are the current agencies using facial recognition or biometric technology.

ASSISTANT COMMISSIONER FOARD: Biometric data, yeah.

COUNCIL MEMBER HANIF: So, aside from these three, agencies are not implementing or making use of biometric tools like ACS, for example? I'm just thinking of an agency that could be.

ASSISTANT COMMISSIONER FOARD: Sure. So, what it means is that those are the agencies that are using biometric data along with data analysis to help support decision-making in a way that has a material impact. So, it is possible that agencies could be using biometric data in different ways that don't meet that entire threshold for reporting under Local Law 35.

COUNCIL MEMBER HANIF: I see.

ASSISTANT COMMISSIONER FOARD: But if an agency, again, is collecting biometric data, that's protected under the Identifying Information Law. So, all the collection, disclosures, and use of that data is still governed by that law.

COUNCIL MEMBER HANIF: Understood. And you said that they're using biometric data. So, are they using a tool themselves, or have they purchased from a third-party company?

ASSISTANT COMMISSIONER FOARD: Sure. So Local Law 35, in general, asks agencies to be clear when a vendor is involved. In about half of the systems reported under the law, do leverage a vendor in some form or another. I do believe that those three do include a vendor. I would have to go back to the report for the specifics.

COUNCIL MEMBER HANIF: Got it. So, you don't have the name of the agency or the vendor right now?

ASSISTANT COMMISSIONER FOARD: I don't have the vendors, no.

COUNCIL MEMBER HANIF: Got it.

I want to pass it to our Public Advocate as soon as he's ready.

PUBLIC ADVOCATE JUMAANE WILLIAMS: Thank you. Good morning, everybody. My name is Jumaane Williams, Public Advocate of the City of New York. I want to thank the Chairs as well as all the Members for holding this important hearing. It's going to be the opening statement in the middle of the hearing, so thank you for giving me the opportunity.

The delicate balance between our civil liberties and our public safety has always been a nuanced conversation, but today we find ourselves at a critical moment where our civil liberties are being eroded faster than ever, with technological advances enabling widespread and pervasive surveillance. New Yorkers are no strangers to surveillance overreaches made in the name of public safety. In the wake of 9/11, we saw how Muslim New Yorkers were profiled and surveilled, sowing fear and distrust amongst our community. Individuals impacted by the abuses of stop-and-frisk policies have continuously had their past records used to increase charges for unrelated crimes even decades later, despite two New York City laws requiring those records to be sealed or destroyed. These same records have contributed to the NYPD's facial recognition database. Transparency and accountability are critical for protecting New Yorkers' civil and constitutional rights.

Thus, New York City must maintain strong enforcement of the Public Oversight of Surveillance Technology Act, or POST Act, or Post Act. In New York City, facial recognition technology has enabled an increasingly expansive and pervasive surveillance network known as the Domain Awareness System, DAS, which, despite its initial launch in 2012, grew rapidly during the previous mayoral administration. Recently, it was announced by NYPD Commissioner Jessica Tisch that the system will be receiving a major upgrade and introducing real-time policing. Understanding how DAS and other surveillance technology have been and will be utilized is critical for addressing gaps in the system as well as abuses of power. The package of bills passed last session are proof of that, and we must build on their foundation.

In addition to maintaining the integrity of the POST Act, the City must regulate the growing data broker economy and implement more robust consumer protection laws, including ways to opt out of data collection. This is particularly important in light of recent news by Meta to integrate facial recognition technology into its smart glasses. These glasses, as well as other video recording devices like a head-mounted GoPro, have already been used by Immigration and Customs Enforcement, ICE officials, to film protestors in several documented cases. The normalization of facial recognition by private and public institutions will only further enable the use of facial recognition tools to identify and surveil individuals and communities, ensuring the abuses of these rogue and mass individuals continue unimpeded. We cannot allow this to become the new norm. Like Pandora's box, this technology may not be something we can go back on, but we are not powerless in regulating either. We have seen the harm of leaving the tech industry to self-regulate in the cases of social media.

Therefore, instead of allowing this technology to grow without guardrails and allowing the creeping erosion of our privacies to further take root, we must be proactive. I'm looking forward to working with the Administration to help curtail overreaches, demystify opaque surveillance technology, and affirm New York's right to privacy, digital or otherwise. I know that this is a tough conversation, and there's been so much wrong identification, particularly the further you were from being a White male because of the data that's been in the system, and part of that means we need more data in the system, but part of that means we have some more problems with the overreaches I've spoken about. So, I'm also trying to figure out how best to work with this technology that's not going away, and I don't think we've quite gotten it right yet so I'm looking forward to these conversations. Thank you.

CHAIRPERSON DE LA ROSA: Thank you, Public Advocate, and if you have questions for the Admin, feel free.

CHAIRPERSON DE LA ROSA: I just want to go back. So, you know, as I mentioned before, the Committee wants to have a good working relationship with the agency, and based on the history here on the record, the Council has asked for what agencies collect biometric information, including fingerprints, iris scan, facial geometry, voice print, and DNA. We haven't received that information. We've asked for it in June and December of last year. I understand that the agency has a Chief Privacy Officer, and that person is not here or not testifying today. Is this information that your Chief Privacy Officer would have?

ASSISTANT COMMISSIONER FOARD: So, for the specifics of how the CPO enforces the local laws, the Identifying Information Law, as well as the policies, I would have to take that back to them to get clarity on their insight into agency data sets. But again, the agencies are responsible for following the Identifying Information Law, whether or not, you know, that data is being shared with other agencies, whatever its use may be. Those laws apply no matter what. My team does not have a sort of central repository of data sets that are collected. We just have visibility into the tools that we described are sort of under that framework.

CHAIRPERSON DE LA ROSA: I get what the law says, but the Council is a partner agency, for lack of a better word and, if the Committee is asking for information, I would think in a collaborative relationship, if that information can be made available, that the agency would make every effort to make it available.

ASSISTANT COMMISSIONER FOARD: I'm happy to take that request back, and as you said, describe whether or not it can, and if so, how.

CHAIRPERSON DE LA ROSA: And we also welcome your Chief Privacy Officer to join you next time. There's plenty of seats and, you know, water and mics, so we're happy to have that person come and share with us what is shareable.

I want to ask about DNA. Public advocate, if you have a question, just let me know. But I did want to ask about DNA. Can you tell us which agencies currently collect DNA?

ASSISTANT COMMISSIONER FOARD: The only one that I'm aware of, as I described previously, is the one that's reported by the Office of the Chief Medical Examiner for their DNA matching. That's the only one that within my purview that I'm aware of.

CHAIRPERSON DE LA ROSA: That's the only one that that has self-reported that they collect DNA.

ASSISTANT COMMISSIONER FOARD: Correct. Under Local Law 35.

CHAIRPERSON DE LA ROSA: Okay. Do any vendors collect DNA on behalf of City agencies?

ASSISTANT COMMISSIONER FOARD: You would have to speak to the specific agencies that are using or potentially collecting that data for the specifics of any vendors.

CHAIRPERSON DE LA ROSA: Okay. Let's see. Okay. I want to ask about, and I'm going to probably mispronounce this, but the Fusus program. That's how you say that? Fusus? In June 2024, Mayor Adams and the NYPD Commissioner announced the Fusus program, a camera integration platform allowing private businesses to voluntarily register and integrate their security cameras with local NYPD precincts. The initial contract was for one year. Is this program still active? At our September 30th hearing, the NYPD confirmed that the program is still active. And if yes, do you have any information about how many businesses have signed up? How can businesses sign up? If not active, why not? And how many crimes have been prevented through the program?

ASSISTANT COMMISSIONER FOARD: I don't have any information about… the Fusus program, you said?

CHAIRPERSON DE LA ROSA: Yeah.

ASSISTANT COMMISSIONER FOARD: Yeah. I'm sorry. I don't have any information about that program.

CHAIRPERSON DE LA ROSA: So, the NYPD does not report to OTI on this program?

ASSISTANT COMMISSIONER FOARD: OTI has not seen Local Law 35 report about that system. So again, I would defer to NYPD about their decisions about what tools do and do not need to be reported under Local Law 35, but there's nothing that OTI has seen.

CHAIRPERSON DE LA ROSA: Okay.

ASSISTANT COMMISSIONER FOARD: My team has seen.

CHAIRPERSON DE LA ROSA: Okay. We'll follow up on that.

And I want to ask about transparency of City surveillance devices. During the de Blasio Administration, the former CTO, John Paul Farmer, announced a plan to label City-owned cameras and devices so that the public could identify whether they're operated by NYPD, DOT, or any other agency. Would your Administration support implementing this level of transparency regarding the ownership and operation of surveillance cameras and related technologies?

ASSISTANT COMMISSIONER FOARD: So, I think if we're talking about the use of cameras more broadly, that affects not only other parts of OTI, but a lot of other agencies. I wouldn't be able to make that decision on behalf of other agencies here at this time. I'm happy to bring conversations together to help talk about them more broadly, but that's not something that I could comment on just on my own.

CHAIRPERSON DE LA ROSA: Okay. Okay. And going into ICE and federal requests and data sharing, if a City agency receives a subpoena from the federal government seeking data, such as biometric information or DNA, what is the City's policy for responding?

ASSISTANT COMMISSIONER FOARD: I would have to defer to both the Law Department and other agencies' legal teams on how they're actually responding to court orders. That's not something that my team oversees.

ASSISTANT COMMISSIONER FOARD: Okay. I'm going to turn it back to Council Member Hanif, who has additional questions.

COUNCIL MEMBER HANIF: Thank you.

So, the FTC's Rite Aid findings show significantly higher error rates for Black and Brown individuals and women. Does OTI consider the deployment of biased, error-prone biometric systems to be a civil rights concern?

ASSISTANT COMMISSIONER FOARD: So, I think the facts that we've all talked about this morning are very real, and they're very in front of us as we think about these technologies. OTI's approach generally with technology, and then specifically AI, is to really think about risk and use in the specific context of where things are being used. As the

Chair's statement said at the top, the technology in and of itself is neither good or bad. It needs to be thought of in the context of use. And so what we want to be able to understand and what we want to be able to work with agencies on is understanding where technology, AI in particular, where it needs to be used, where an agency is perceiving a need, and understanding how it would be used and what sort of risks could be brought to bear by using it in that context, and then through the requirements of the new office.

COUNCIL MEMBER HANIF: And that's what OTI does, like guides an agency.

ASSISTANT COMMISSIONER FOARD: We guide citywide direction and policy in the use of AI.

COUNCIL MEMBER HANIF: Could you walk me through, like, guiding the NYPD on their choice of biometric data?

ASSISTANT COMMISSIONER FOARD: Sure. So, some of this is in flux now because of the new laws that we mentioned. So those will take effect in June of this year, and then a lot of the work that is the core sort of policymaking around pre-deployment risk and management will move to that office.

COUNCIL MEMBER HANIF: Got it. You can just talk about what's happening right now.

ASSISTANT COMMISSIONER FOARD: What we do right now is we work with agencies on an advisory basis and provide them with both written guidance and then one-on-one guidance as needed to talk about where they are interested in technology, particularly emerging technology, particularly AI. That takes place across different parts of the life cycle. So sometimes agencies are sort of at the very beginning of trying to think through problem solving and they just want to brainstorm. In other instances, they're looking for maybe some guidance around procurement or the sorts of things that could help them make a more concrete decision. So, we work with them, like I said, on either a one-on-one basis. We also have written guidance that we provide agencies. We have a document that we call our AI Principles, which is a publicly available document. It has the City's five AI principles, trust and transparency, validity and reliability, social responsibility, information, privacy, and cybersecurity. And so, our goal is to anchor agencies' use of AI in those five principles and to help them steer their work in that direction.

COUNCIL MEMBER HANIF: So, then specifically on biometric technologies, is that just a piece of the larger work that OTI is guiding agencies around?

ASSISTANT COMMISSIONER FOARD: That's exactly right. So, identifying information, biometric data, all of this would be part of a broader ecosystem of understanding risk and doing a cost benefit when it comes to thinking about AI.

COUNCIL MEMBER HANIF: And then does the City have visibility into whether private retailers share biometric data with federal innovation authorities?

ASSISTANT COMMISSIONER FOARD: OTI would not have any visibility into that. We don't have a role with regulating the private sector.

COUNCIL MEMBER HANIF: Understood. And then curious about both of them, Intro. 213 and 428, around enforcement tools that would be used to effectively investigate violations.

ASSISTANT COMMISSIONER FOARD: Okay. So, I could say more generally, since OTI does not have regulatory sort of authority over the private sector, we wouldn't be driving enforcement of any private sector regulation. We are equipped and able and ready to support agencies in their work and what they do. So, if agencies are either considering technology for their own use or understanding the role that technology plays in the day-to-day work that they're doing, OTI is available to support on a technical assistance front.

COUNCIL MEMBER HANIF: And then going back to the agencies, if there's a data breach, do you also, are you troubleshooting, problem solving?

ASSISTANT COMMISSIONER FOARD: There are other parts of OTI, the Office of Information Privacy, which we've talked about, Cyber Commands, those are the groups that are involved when issues of data breach come up. I would defer the specifics to them. They're the ones who can talk through the specifics of those processes.

COUNCIL MEMBER HANIF: I'll pass it back.

CHAIRPERSON DE LA ROSA: Thank you. Public Advocate.

PUBLIC ADVOCATE JUMAANE WILLIAMS: Thank you so much, Madam Chair.

I just have a couple of questions. Two questions, actually. I don't know if they've been asked before, but what contracts does the City currently have regarding facial recognition?

ASSISTANT COMMISSIONER FOARD: The ones that we would be aware of are the ones that are reported under Local Law 35. There's two agencies who currently report. The most recent report, I should say, is 2024's report. 2025 will be published by the end of this month. Under the 2024 report, there's two agencies who report the use of facial recognition. I don't have the specific vendors in front of me, but for the most part, that's asked as part of the Local Law 35 reporting.

PUBLIC ADVOCATE JUMAANE WILLIAMS: Okay. Can we get that? I know it's Local Law, but I'd love to just get it in one place, if possible.

And I know that many private businesses use facial recognition technology to crack down on shoplifting and other things, but I'm wondering what standards are currently in place to regulate how those businesses use those tools? Is there a set number of days that they're required to keep the footage? Are they supposed to have signage? Stuff like that.

ASSISTANT COMMISSIONER FOARD: I, again, don't have a global view into that. I think we have some familiarity with, I believe it's Local Law 3 that requires the signage, which I think is what you're referring to. I don't know the specifics of retention, if there's any requirements on retention within that law. OTI doesn't have direct management of any private sector actors, so we don't, sort of on a day-to-day, get involved in that sort of issue. The Office of Information Privacy would be involved for City collection, so if a City agency is collecting and maintaining those data.

PUBLIC ADVOCATE JUMAANE WILLIAMS: Who would have oversight of the private stuff that's happening?

ASSISTANT COMMISSIONER FOARD: I would imagine that's probably policy area specific. I don't have a full picture of that. I think it would depend on what part of the private sector is being discussed. And again, OTI is able to support any agency who's trying to do work involving the private sector to provide that sort of technical expertise for it, but we wouldn't be the drivers of any of that regulation.

PUBLIC ADVOCATE JUMAANE WILLIAMS: So we may not have any real policy or laws covering data collection from private actors?

ASSISTANT COMMISSIONER FOARD: OTI is not involved in any such laws.

PUBLIC ADVOCATE JUMAANE WILLIAMS: I'm going to tell you now that the City doesn't have any either.

ASSISTANT COMMISSIONER FOARD: I would hesitate to speak on behalf of the whole City, but just from OTI's position, I don't think we've got any involvement in that sort of framework.

PUBLIC ADVOCATE JUMAANE WILLIAMS: Okay. So, from your knowledge and OTI's knowledge, it's probably not, so these folks can be collecting this information and we have no idea what they're doing with it.

ASSISTANT COMMISSIONER FOARD: To the best of my knowledge, yeah, I'm not aware of OTI for sure, and I can't speak more broadly to City-wide practice.

PUBLIC ADVOCATE JUMAANE WILLIAMS: Thank you. And then you may have spoken about this before, but in terms of the data in that, you know, makes some bad data out, what are we doing to balance that out? Because I know, you know, the data's primarily from, this is for facial recognition, primarily cisgender White men, and it's sort of the rate of wrong, what's the word, getting the wrong person. I forgot the…

CHAIRPERSON DE LA ROSA: Misidentification.

PUBLIC ADVOCATE JUMAANE WILLIAMS: Misidentification. Thank you very much. So, the misidentification rate is high when it goes beyond that, so what's being done to try to change?

ASSISTANT COMMISSIONER FOARD: Yeah. That's a great question. So, from the perspective of facial recognition technology, as the Chair said in her opening statement, the technology has come a long way over the past couple years in terms of accuracy rates, but what you're describing is often still present. There do tend to be issues in sort of less perfect sort of settings, you know, photos that aren't taking in a higher controlled environment, as well as potential differences across groups. When we take that sort of conversation more broadly and thinking about it from the perspective of City agencies, and to the extent that we're talking about the use of this sort of data in sort of an AI setting, the important thing for us to be thinking about, as Council Member Hanif said earlier, is the sort of role of that use of that data in the broader picture for risk and management of that technology. So, every, you know, use of technology, every dataset has its own sort of flavor of risk, sometimes less, sometimes more, depends on the use, depends on the agency, depends on, you know, what exactly is being collected. We tend to focus on not a sort of single broad brush, but instead a use case specific approach to say, how are these data being used in this context, with which technology, by which agency, for what purpose, and really to drill in on the specifics of use. So, that risk profile looks really different from one place to the next, and our effort at OTI is often focused on understanding that risk profile within that specific context.

PUBLIC ADVOCATE JUMAANE WILLIAMS: Do you have that conversation with NYPD, and how does that go? How's their misidentification rate been going, and have you been able to help them address that?

ASSISTANT COMMISSIONER FOARD: We haven't had that specific conversation with NYPD. The work that we do currently is on an advisory basis, but when the new local laws take effect in June of this year, the GUARD Act and the new Office of Algorithmic Accountability, pre-deployment assessments will be required for these sorts of tools, and so that would be a more formal mandated program going forward.

PUBLIC ADVOCATE JUMAANE WILLIAMS: All right. And it would have been great to do it even without the formal, because I think that's one area that can cause a lot of harm, so those kind of conversations would have been great, even beforehand.

ASSISTANT COMMISSIONER FOARD: Of course.

PUBLIC ADVOCATE JUMAANE WILLIAMS: You know, this is a new Administration since the last one.

But the last question is, just with things like ChatGPT and other AI tools, is there some kind of regulation for agencies in general, how and when they can use it, and their employees can?

ASSISTANT COMMISSIONER FOARD: Yeah. So, there's a sort of ecosystem of governance around tools like that. In general, of course, agencies should only be using tools that have been approved by their agencies for use, so often that is something that an agency's cyber officer is going to be looking at, or information security officer, their legal, their agency privacy officers, etc., to help assess the appropriateness of a tool within its use. More generally, OTI has guidance for agencies on generative AI tools in particular. It's a sort of collection of best practices, what to be mindful of, what to be wary of, and then where we think agencies could be doing some more work with those sorts of tools. So, I would describe it as a collection of support that agencies have to use those tools.

PUBLIC ADVOCATE JUMAANE WILLIAMS: Thank you. Thank you, Madam Chair.

CHAIRPERSON DE LA ROSA: Thank you. I don't mean to be antagonistic, but I do need to say this, because if not, I will explode. Listen. I think that I understand that we have been appointed a new Chief Technology Officer. When I think about Chief Technology Officer, I think about citywide. So, I understand she's not here today. Today's her first day, and I appreciate y'all coming, and being here, and testifying. But I want to set the expectation that this Committee is going to ask you all about citywide positions on things, because OTI has a directive to sort of be the clearinghouse for how technology is used across the City, and what we have seen here today is the inability for OTI to answer very basic questions that are policy positions that an agency should have clear. So, we're going to give you sort of a fresh start and say, going forward, we hope that the Chief Technology Officer can join us here, and that we can clearly know what are the positions on things, for example, like the Public Advocate asked about, how are we dealing with industry? How are we dealing with the private sector? How are we dealing with agencies that are not compliant? How are we dealing with agencies that are not willing to give us information? It is our expectation that here in this Committee we can dig into that, because today we haven't been able to do that. And I understand we're in a transition phase. It's only March. We're going to be cognizant of that and understand that that is the reality. But we want to make sure that going forward we have the information. And if this Council asks for information, that if the information can be made available, and it is information that by law we should have, or by collaboration we should have, that

that information be made available, because it's only going to help us to legislate better, right? If we don't know what's happening across the board, then we're going to continue to put in local laws, and then you all are going to have to be tasked with implementing those local laws when you could have just given us the information, we could have dissected that information and see where we need the local laws, and so it's important for the collaboration between the Council and the agencies that we have the information that we're asking for. We're going to write a letter following this hearing to ask for specific data sets. We ask that if there are things you can give us, give them to us. And if there aren't things that we can give them, then we could have that conversation on the side.

I do want to ask a question of HPD. So unlike Intro. 213-A, which is enforced by a private right of action, Intro. 428 does not clearly state the enforcement mechanism. In your opinion, what would be the best enforcement mechanism, and what is your opinion of whether HPD should enforce that law?

DEPUTY COMMISSIONER JOFFE: Thank you for that question. So, in terms of, I'll focus on what we think makes the most sense here. I did talk about the important role HPD plays in terms of education and ensuring that both tenants and owners understand their rights, and no law can meaningfully be implemented without that so we do see that as incredibly critical here. The private right of action, we also do think is as well. There are parts of this that are quite complicated, but in which a tenant might have concerns that they should be able to take to court so we also think that's an important part of the infrastructure here. We're open to discussing more about the actual, our initial interpretation of what the law does require, but also what the Council would like to see here. We want to be a good partner. This is an area of technology that we are not expert in and it is evolving and we understand that, but we would love to work together to figure out the right path.

CHAIRPERSON DE LA ROSA: Yeah. Definitely, we should have a conversation offline about it because I think that education is important. It's always important anytime we pass a law that people know how to follow the law, but I also think in my interpretation that HPD has a responsibility to also implement the law and enforce the law, and so we should have that conversation about what that looks like.

Did you have any other questions?

COUNCIL MEMBER HANIF: I want to go back to OTI and understand, do you all give your analysis? I know it seems as though the biometric tools technology are neutral. You don't see them as, you know, this specific vendor has data that was leaked and someone who doesn't even live in the city was charged with a criminal case. Like, are you all deciding or assessing, like, here's what you need to know about the vendor and then the agencies select the vendor?

ASSISTANT COMMISSIONER FOARD: So, what you're pointing to, I think, are questions that are asked in different parts of the technology lifecycle by different groups. So, when we think about, you know, using vendors and using technology that's procured, obviously there are sort of factors there that are unrelated to my team, for example, in cybersecurity and procurement.

COUNCIL MEMBER HANIF: So, OTI doesn't do that, but you're saying there's another crew?

ASSISTANT COMMISSIONER FOARD: So, I'm saying I think that vendor risk would be something that more than one group would cover when thinking about the sort of role that those decisions play in purchasing technology. Certainly, understanding the factors related to engaging with a vendor are valid risks to be considering for procurement. Some of those frameworks would be outside of my remit, so I don't want to speak to some of the specific controls.

COUNCIL MEMBER HANIF: But are you saying that somebody does that?

ASSISTANT COMMISSIONER FOARD: There are many review processes for agency procurements that would include understanding the vendor involved.

COUNCIL MEMBER HANIF: Could be that one agency is using a vendor that has a bad reputation or has wrongfully charged or gotten someone arrested?

ASSISTANT COMMISSIONER FOARD: I can't speak to those particular criteria. I will say, you know, there are frameworks, for example, on protecting data that our cybersecurity office, the Office of Cyber Command oversees, for example, to make sure that data are, you know, housed within the U.S. and have other sorts of protections that are used as sort of baseline measurements for security, and then other factors could come into play in terms of how vendors are being assessed. Those particular criteria would not be ones that I'm exactly familiar with.

COUNCIL MEMBER HANIF: But knowing that technology performs unequally across race and gender, should the City view that as discriminatory? What I'm trying to get at is that it seems as though, and this is also not a bad thing, that the City right now does not have a good grasp of biometric technology, and I think taking a neutral position is quite dangerous for our city, particularly because the field of biometrics is only growing. And I take a lot of concern knowing that the NYPD is using this data. I mean, I think we all know anecdotally that they use some kind of data. But I would like to see our City be more involved in not only just making sure a vendor is protecting one's data, but also understanding where that data is being shared, how that data is being used, and then if the data has a breach, that there are some steps to take in response and not work with that vendor.

ASSISTANT COMMISSIONER FOARD: Yeah. So, I do want to be clear that the City has incredibly robust cybersecurity and information privacy offices that exist in City Charter. They are part of OTI so their mandate is to protect data that is collected by the City. The reason I can't speak to the specifics of some of their practices is because I'm not deeply involved in those, and I don't want to misrepresent some of their actual procedures, but the City's data is protected in very robust and strong ways. Agencies have obligations to protect their own data, as we've talked about. And then OTI has, as we've talked about, oversight through its Office of Information Privacy, Cyber Command, etc., over agency activities. Some of the characteristics that you're talking about of facial recognition, which move more from just sort of collection of data into usage of data, particularly in the context of AI, that is an area where we are expanding and building out our processes, as I described. So, the new office, when that takes effect later this year, will have this pre-deployment risk assessment mandate to actually conduct those for tools coming in the door. And vendor accuracy, all of these are factors that are important, part of that conversation.

COUNCIL MEMBER HANIF: But that's not happening right now. I just want to understand what's happening right now, so that we're able to, as legislators, think about where we're headed.

ASSISTANT COMMISSIONER FOARD: Of course.

COUNCIL MEMBER HANIF: I have a question for HPD. So, what do you assess of biometric technology when it comes to tenants with disabilities?

DEPUTY COMMISSIONER JOFFE: Sorry. What do we assess?

COUNCIL MEMBER HANIF: Could reliance on flawed biometric systems increase the risk of wrongful lockouts, or make one population more vulnerable than the other? I'm speaking about people with disabilities.

DEPUTY COMMISSIONER JOFFE: Thank you for the additional context. We are certainly not the experts in this technology, but as we discussed, we have concerns related to the use and misuse of any of this data, and absolutely any vulnerable or at-risk population is going to be more at risk. I don't know that I could foresee all of the ways in which people with disabilities might be impacted, but I certainly imagine that New Yorkers living with disabilities might have additional concerns about their personal data being shared publicly.

COUNCIL MEMBER HANIF: And then at the moment, does HPD collect or know about property owners who are using this kind of technology?

DEPUTY COMMISSIONER JOFFE: Local Law 63 is the baseline. This law would add to that. That, I think, is how we would start to know the full scope. Well, I guess we would prohibit the use of it. But so without this law, we don't have necessarily good insight into what private market actors are doing yet.

COUNCIL MEMBER HANIF: Got it. So, what about through 3-1-1? Like, could there be complaints that are being tagged right now as, okay, this property owner uses this technology, and tenants are fighting against installation, which I know has happened in the past in our city?

DEPUTY COMMISSIONER JOFFE: Yes. Absolutely, tenants could call 3-1-1 and have concerns and express those concerns. Local law 63 and no law currently bans the technology, so the City wouldn't have something to do in response, nor would a tenant necessarily be able to bring a claim unless there was some other law that it was violating, which is the space in the existing regulatory infrastructure that this bill would be filling.

COUNCIL MEMBER HANIF: Thank you.

CHAIRPERSON DE LA ROSA: Who is HPD's technology person?

DEPUTY COMMISSIONER JOFFE: We have a Deputy Commissioner for Technology at HPD.

CHAIRPERSON DE LA ROSA: Okay. And what is that person's main responsibility?

DEPUTY COMMISSIONER JOFFE: Sorry. I did not come prepared to discuss Prashant's full range of technology, but, or full range of responsibilities. So, apologies to Prashant if he's watching and I misstate any of this, but he oversees a team of people at HPD who works with us on all of our technology needs, and so that includes everything from our cell phones, our computer access, every time I accidentally lock myself out, too, we are exploring new and robust software. And then, you know, if I were to have questions about new or emerging technology, I would certainly go to him and his team, and I imagine he would work with others across the City depending on the nature of the request.

CHAIRPERSON DE LA ROSA: And does he play a role in, like, the compliance of this type of laws that now the Council is looking to pass?

DEPUTY COMMISSIONER JOFFE: As structured, I'm not sure that he would. It would be the team that gets involved in Local Law 63 is our Enforcement and Neighborhood Services Team. They certainly could and would consult with him on any technology aspects of it, and this is not an area that HPD necessarily has, you know, robust experience in, so we certainly would be leaning on our technology-oriented folks, both those who are at the agency at OTI for any support, but it would be primarily through our enforcement team that we would be engaging in this area.

CHAIRPERSON DE LA ROSA: And then who in the agency engages then with OTI if there's a need?

DEPUTY COMMISSIONER JOFFE: Certainly, the Deputy Commissioner would, but other parts of the agency will as well, depending on what we're talking about, if there's an issue about data collection or, you know, individual projects, we're certainly an agency that works across, and so that could be running through multiple parts of the agency, and we have a separate Chief Privacy Officer as well.

CHAIRPERSON DE LA ROSA: Great. I don't mean to put you on the spot. I'm sorry. I just wanted to ask because it's interesting for me to see, like, an agency that isn't necessarily technologically heavy or inclined, right, but you're here in the Technology Committee because there is the laws that are now going to be passing through this Council that are going to be speaking to data collection in agencies that we don't even think, you know, are talking about technology on an everyday basis, so what we're trying to reconcile on this side is, like, then how does that communication happen with OTI?

DEPUTY COMMISSIONER JOFFE: Absolutely. Yeah.

ASSISTANT COMMISSIONER FOARD: I can weigh in on this as well, so I think actually what you're getting at is exactly what's happening more and more, which is that you need more than one agency to come together to bring the full suite of expertise. We at OTI know a lot about AI, but we don't know about the details of housing policy and vice versa. Well, sorry, I shouldn't say it. I'm sure there are very smart people at HPD who know a lot about AI, but they don't necessarily have a citywide mandate to understand AI issues, so we are at OTI more than prepared to be able to work with agencies to understand where, you know, regulation, sort of public discussions around policy relate to technology but aren't solely about technology, right? Instead, it's involved in some other policymaking component, so that is where OTI plus an agency partner make the best sort of complement that you have to then be able to address some of those issues. And to your point earlier around, you know, OTI's ability to answer some of the questions that you've had, you know, we have the ability to work with agencies within the confines of our authority. We have the ability to work with agencies as the City's central technology officer, but agencies themselves also hold on to some of that decision-making authority as well, so our balance is to say how can we support agencies in doing the core mission that they need to get out the door, and then where are we thinking about citywide issues that do require a little bit more of a central coordination, and that's where OTI can also step in.

CHAIRPERSON DE LA ROSA: Yeah. And I completely understand that. I think that it's one thing to offer support, which is amazing and necessary, but when we're talking about emerging technologies that are then infringing on people's civil rights and privacy, then there has to be a level of enforcement, right, and so I think as the Chair of this Committee, what I'm interested in is figuring out where is there an enforcement mechanism or place, and where does it live? Does it live in OTI? Does it live somewhere else? Like, that's sort of, I think, at the crux of some of what may seem like frustration. It's not frustration. It's more like we're tasked with making sure that people's privacy in New York City is protected, right, and so we got to figure out where the firewalls are and where enforcement lives if there's agencies that we know. I mean, you know, the new DOCS Commissioner is a friend, someone I admire. I think he's going to do an amazing job, but agencies outlive leaders, and so if there's an agency that hasn't been compliant with something and there's a lawsuit in place because they haven't been compliant in something, then we have to make sure as a Council that we're using our oversight authority to make sure that that compliance happens, and so where are the teeth? Like, from where do we get the enforcement juice, you know?

ASSISTANT COMMISSIONER FOARD: Yeah. I think it's a very important question, and I think in some parts of OTI, again, like cybersecurity and information privacy, there's a decently long history of enforcement as defined in those frameworks for those particular areas. As we move to the summer with the introduction of the Office of Algorithmic Accountability, that's where this conversation, as it relates to AI, will start to take better shape because that will have much more specificity in terms of the actual requirements. A lot of what we've been doing on a more, I would sort of describe it as an advisory basis right now, is sort of the precursor to being able to stand up those requirements later this year.

COUNCIL MEMBER HANIF: Do you know if any independent audits have taken place of City agencies that use data?

ASSISTANT COMMISSIONER FOARD: That use data? So, I mean, in the broadest of terms, I would… if the question is about whether or not there are any audits that have taken place on the use of biometric data, is that the question?

COUNCIL MEMBER HANIF: Yeah.

ASSISTANT COMMISSIONER FOARD: I don't have any awareness into that in terms of the specific. That could also be very unrelated to technology. It would depend on what sort of audit I think you're thinking about.

COUNCIL MEMBER HANIF: Well, the ones that you help assess NYPD and the Chief Medical Examiner to host in their agency.

ASSISTANT COMMISSIONER FOARD: OTI has not been involved in any audits on those specific tools. I don't think we've been involved in anything under Local Law 35 at all.

COUNCIL MEMBER HANIF: Got it. And then what is OTI's position on the two legislation?

ASSISTANT COMMISSIONER FOARD: I'm sorry.

COUNCIL MEMBER HANIF: On the two legislation that we're hearing?

ASSISTANT COMMISSIONER FOARD: We're largely deferring to DCWP and HPD here. Again, you know, as we were just talking about, we want to make sure that the subject matter experts on the policy area are the ones leading the conversation. OTI is available to support on implementation for laws like this if there's a technical need from the agency, but we don't have enough insight into the existing regulatory work that these agencies do, so we defer to them on that.

COUNCIL MEMBER HANIF: Got it. So that does pose a big challenge, I think, if we're relying on the other agencies for their policy expertise and then OTI remains neutral on how you view these tools.

ASSISTANT COMMISSIONER FOARD: I would probably say that we are not neutral on how we use the tools. We need to work with the agencies in the context of what they're trying to do and what they're being asked to do. So, if an agency came to us and said, you know, we need to sort of implement a prohibition on this technology, we can't be neutral on that outcome because that outcome has already been described, and so we're there to provide from a technical perspective what is needed to be able to fill in the know-how gaps, essentially, there. We think about technology from the perspective of risk management and understanding where particular uses of technology, again, look very different in different contexts, and so we want to be able to say we're coming in with an awareness that there can be positive impacts, there can be negative impacts, and we have to weigh all of those things together and then understand even often what is the impact of not acting as well, which is another variable that comes in. So, you know, our goal is to be able to support agencies in what they need to do on a day-to-day basis. We describe ourselves as a service agency with other agencies as our clients, and so we need to let them tell us what the issues are, what they're trying to solve, so that we can plug in in the right way.

COUNCIL MEMBER HANIF: That makes sense. I have a better understanding of how OTI operates. I appreciate it. Thank you.

ASSISTANT COMMISSIONER FOARD: Thank you.

CHAIRPERSON DE LA ROSA: We got testimony from DCWP. Would you all be willing to read it on the record on behalf of DCWP?

ASSISTANT COMMISSIONER FOARD: I'm only able to speak on behalf of OTI today.

CHAIRPERSON DE LA ROSA: Okay. All right.

I want to ask about data collection and data brokers. Does New York City or any City agency purchase data about individuals from private companies?

ASSISTANT COMMISSIONER FOARD: I don't have any awareness of that myself. I would have to bring in other parts of either OTI or potentially even some City agencies to get you a fuller answer.

CHAIRPERSON DE LA ROSA: Is there a unit or a part of OTI that deals with data collection and data brokers in general?

ASSISTANT COMMISSIONER FOARD: On data collection, there would be, again, multiple parts of the City that focus on data collection, Office of Information Privacy, Office of Data Analytics, which is also part of OTI. These are groups who have responsibilities related to data collection writ large. In terms of purchasing data, I think we certainly could talk to the Office of Data Analytics and others, but I'm not sure if there would be others who would need to get pulled into that as well.

CHAIRPERSON DE LA ROSA: Okay. I guess the same answer, but do you know if any New York City agencies purchase data from or sells data to data brokers, including biometric data?

ASSISTANT COMMISSIONER FOARD: I don't have the answer to that.

CHAIRPERSON DE LA ROSA: Okay. And then in terms of facial recognition, what steps is OTI taking to ensure that facial recognition technology systems used by the City are accurate across demographic groups?

ASSISTANT COMMISSIONER FOARD: So, this gets back to what we were talking about in terms of our evolving work, working with agencies to better understand the impacts of their technologies, risk management, etc. We haven't had direct conversations with any agencies yet about facial recognition, but as we move to the summer, the new office will have a sort of more clear mandate about how it engages with agencies about this.

CHAIRPERSON DE LA ROSA: Does OTI require vendors to submit their algorithms to the National Institute of Standards and Technology or face recognition vendor test program?

ASSISTANT COMMISSIONER FOARD: I'm not aware of any requirements. My understanding is that most vendors do that on their own, so that they have those data points to be able to point to.

CHAIRPERSON DE LA ROSA: Do you know what documentation vendors must provide to demonstrate accuracy and reliability of their systems?

ASSISTANT COMMISSIONER FOARD: So, if we're thinking about this within the context of AI, that, again, I think is where we'll see more formalized policymaking later this summer that will speak to how agencies are working with vendors and factoring in issues of bias and accuracy. So right now, I think most of that would be raised under the context of other frameworks for helping to govern the use of that technology, whether cybersecurity, privacy, or otherwise.

CHAIRPERSON DE LA ROSA: Okay. That's it for me. Do you have anything else? No?

Thank you all for coming. I do want to say that DCWP did submit testimony for the record, and we'll put it up with the documents online, and we thank you for coming, and we look forward to continuing the conversation.

Also want to acknowledge that Council Member Won joined us virtually earlier.

Thank you. Thank you for coming.

Okay. I now open the hearing for public testimony.

I remind members of the public that this is a formal government proceeding, and the 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 the transcript of such recording to the Sergeant-at-Arms for inclusion in the 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 three minutes to speak on today's topic on facial recognition technology and the collection of biometric information, as well as Intro. 213-A and 428.

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

All right. So, we're going to call up our next panel, and I apologize for the names. If I get them wrong, please correct them for the record, but it says Nina Lashkajian, Laura Moraff, and Talia Kamran.

You may begin whenever you're ready, and just please correct the names for the record.

LAURA MORAFF: Good morning. My name is Laura Moraff. I'm a Staff Attorney at the Legal Aid Society's Digital Forensics Unit, and I want to thank Chair De La Rosa and the Committee Members for the opportunity to testify this morning.

I want to start by talking a little bit more about the technical limitations of facial recognition technology. There's already been discussion this morning about the racial and gender biases baked into facial recognition technology, which is, of course, a very real problem. It's also less accurate for elderly individuals as well as children, and I also want to highlight that facial recognition technology also fails to recognize people with facial differences and various conditions affecting people's facial appearance a lot of the time. Council Member Hanif, if you had asked about concerns for tenants with disabilities, and this is definitely a concern that's highlighted in a Wired article from last year, when face recognition doesn't know your face is a face. And then there are also similar accuracy issues with other forms of biometric technology. There have been studies finding that iris recognition and voice recognition are less reliable for women. Voice recognition also may be less reliable for people with accents underrepresented in the system's training data, and speech features can change with age, sickness, exhaustion, and tension, which makes identity verification based on voice prints challenging and potentially inaccurate as well. And the biases in facial recognition technology and other forms of biometric recognition technology lead to very real harms. I work in a public defender's office, and we see far too many cases of people being arrested because of faulty facial recognition technology matches. Many of these cases never make it into the public discourse because people may not want to relive the worst days of their lives in the media, or the case gets dismissed before we get enough information to present it in that way. But last year, we had a client, Trevis Williams, who was arrested based on a facial recognition match, even though he was eight inches taller, 70 pounds heavier than the person the NYPD was actually looking for, but both of these men were Black and wore their hair in braids, and so Mr. Williams spent over two days in jail for an alleged crime that occurred in Manhattan while he was working in Connecticut. We know of three wrongful arrests in Detroit alone, two Black fathers and one woman, Porcha Woodruff, who was wrongfully arrested and held in jail for 11 hours while she was eight months pregnant. And just last week, the Guardian reported that a South Asian software engineer in the UK was arrested because facial recognition technology erroneously matched him with footage of a suspect who was noticeably younger and had visibly different features. Unfortunately, there are more wrongful arrests than I have time to cover in my three minutes, so I'll refer to my written testimony. But I also just want to highlight that you heard in OTI's testimony that every data set or technology has its own set of risks. The risks here are really unacceptable. Wrongful arrests, being flagged as a shoplifter and followed in a store, being blocked from your own apartment building. When this is you, it's really devastating, and the personal and professional consequences of this really can't be overstated. Chair De La Rosa, you were also interested in which agencies are using this technology. Part of the reason we believe a full government ban is necessary in addition to the bills here is because once an agency (TIMER CHIME) has this technology, it's really easy for them to share it with other agencies. I'll refer to a case Legal Aid had last year where the FDNY was using facial recognition technology to identify a protester and then share that with the NYPD. And I know my time is up, so I just want to thank you for the hearing on these two bills, and we urge the Council to pass Intro. 213, Intro. 428, and to introduce (INAUDIBLE) in government use of technology.

CHAIRPERSON DE LA ROSA: Sorry that it's just three minutes. I am grateful that you have such like a wealth of testimony here. I'm looking forward to reading it and continuing the conversation.

NINA LASHKAJIAN: Okay. Good morning, Chair De La Rosa and Members of the Committee on Technology. Thank you so much for convening this important oversight hearing and for the opportunity to testify. My name is Nina Lashkajian, and I am the Technology and Racial Justice Collaborative Fellow at the Center on Race, Inequality, and the Law at NYU Law.

The Center strongly urges the passage of Intros 213 and 428. Facial recognition systems have repeatedly misidentified Black and Brown people at significantly higher rates, yet are deployed in everyday spaces in our city with insufficient oversight and accountability. To allow this technology to operate in essential businesses and our places of residence invites discrimination at scale, and policymakers have a responsibility to prevent tools with known racial bias from causing harm. And this bias is really baked into the technology itself. When systems are trained on data sets in which faces of color are underrepresented, this leads to a higher likelihood that Black and Brown New Yorkers will be misidentified and subjected to harmful consequences. Research has repeatedly confirmed this algorithmic bias, finding that Black and Asian faces are between 10 and 100 times likelier to be misidentified than White male faces. And as Laura correctly outlined, the vast majority of known wrongful arrests due to this technology have been of Black men and women. This is why the Council must pass the two bills on the agenda today and go further by introducing and passing a government ban as well.

Intro. 213 is needed because New Yorkers deserve the ability to partake in everyday life, simple trips to the grocery store, nights out at a concert, without being subjected to intrusive indiscriminatory surveillance. But right now, grocery stores across our city are subjecting customers to biometric recognition as a condition of entry. As a sanctuary city, we cannot allow for the possibility that Wegmans or other retailers could be using this technology to assist federal immigration agents. Passing Intro. 213 is necessary to protect our immigrant neighbors.

Intro. 428 is also a much-needed protection. Our homes should be where we all enjoy the fullest freedom of movement and highest levels of privacy, not testing grounds for biometric surveillance technologies. Unfortunately, we've seen landlords already weaponizing this tech in cruel ways, including to evict tenants for minor violations or to justify rent increases. In Massachusetts, a single mother was evicted from public housing because the technology flagged her for violating a guest policy, only because her ex-husband was routinely coming over to watch their child while she attended night classes.

These two bills are strong, much-needed protections, and the city Council must pass them. The Council should also, as I said, go further by implementing a full ban on police and government use of facial recognition in New York City. In so doing, we have the chance to honor the City's commitments as a sanctuary city and protect all New Yorkers, particularly New Yorkers of color, from harm. I've submitted written testimony as well, and I welcome any questions. Thank you so much.

TALIA KAMRAN: Good morning. My name is Talia Kamran, and I'm a Staff Attorney with the Seizure and Surveillance Defense Project at Brooklyn Defenders. Thank you to Chair De La Rosa and the

Committee on Technology for holding this hearing today.

BDS supports Introduction 428 and 213. These bills recognize the urgent reality that the use of biometric surveillance technology in daily life activities, like entering your home or going grocery shopping, aren't just neutral innovations that can be imposed on the public without regulation. Biometric surveillance systems are essentially artificial intelligence tools, and like all AI, they have to be trained by accumulating an immense amount of personal data, and the more data that they consume, the more powerful and invasive they become. And the risks go further than just the severe evasion of privacy. Facial recognition technology has been widely documented as racially biased and unreliable, particularly for people of color and women, as the Council Members today have pointed out with the Rite Aid example. So, while BDS supports these bills, they only address the private sector's use of biometric recognition technology, but the reality is that the single biggest user of biometric identification technology and other AI surveillance tools in New York is our government, and specifically the NYPD.

New York City has spent billions over the last two decades building a vast surveillance infrastructure embedded in the criminal legal system, the family separation system, and increasingly in other City services. And as public defenders, we have seen these tools deployed against people we represent seeking unemployment benefits, facing evictions, or calling their loved ones from detention. As the Committee mentioned this morning, Securus, the company that provides phone calls to jail and prison inmates, uses an AI-enabled software that extracts and stores voice prints, a form of biometric data from anyone who uses the system, not just people in custody. And beyond biometric data, Securus integrates tools such as Threads, which collects other personal data and uses algorithms to track social networks inside and outside of prisons, often leading to the surveillance of people outside of the criminal legal system who wouldn't otherwise be under investigation. OTI pointed out this morning that the risks of AI-powered surveillance tools lies in how they're used, and it's important in this context to point out that all of the surveillance tools used throughout the criminal legal system work to exacerbate disproportionate surveillance and criminalization of communities of color. In the case of jail calls, more than 80 percent of those detained are being held pre-trial. They've not been convicted of anything and are predominantly being held because they can't afford bail. And those held pre-trial are 90 percent Black and Brown people so the majority of biometric and social network data accumulated is coming from communities of color and is being used to drive the over-policing of those same communities.

Most importantly, there's a trend here. We are playing surveillance whack-a-mole to try to preserve people's constitutional rights and general privacy. In addition to the bills presented today, BDS calls on City Council to pass the ECHOES Act as well as Introduction 820 to abolish the NYPD gang database. And finally, it is imperative that New York implement comprehensive data privacy legislation that understands that personal data is not a commodity that can be freely bought and sold, and most importantly, cannot be collected and weaponized by the government and particularly the police outside of constitutional bounds. Thank you.

CHAIRPERSON DE LA ROSA: Thank you. I just have a quick question and then I'll pass it to Council Member Hanif.

What reasonable safeguards, in your expert opinion, should be applied to you to the use of facial recognition technology?

LAURA MORAFF: I can start and just say that part of the reason that we're really calling for a ban here is because we've seen that, you know, the NYPD has a policy on facial recognition technology and we've seen them circumvent it time and time again. And I started to mention one example of a protester that the FDNY identified and essentially outside of any formal process just emailed it to the NYPD saying, you know, they ran it through their facial. It turned out to be Clearview AI. The NYPD doing that would have violated its own policy, but, you know, we're seeing this over and over, just trying to get around these rules, and so I think we've seen that those guardrails really aren't enough and that's why we're calling for a full ban.

NINA LASHKAJIAN: Yeah. I would reiterate the same answer. Safeguards in and of themselves aren't going to be sufficient to protect New Yorkers, but at the bare minimum we need transparency from City agencies, and also we need to mandate transparency from private actors if they're using this technology. And in our opinion, that transparency should definitely include any disparate impact of the technology. You emphasized, Council Member Hanif, the Rite Aid example, and in that case the FTC found that Rite Aid was not sufficiently accounting for, you know, where they placed this technology, choosing specific stores to place it in. And in fact, their policy ended up having a disproportionate impact by placing the technology more in stores that were within communities of color. So, at the very least, safeguards would have to include auditing for disparate impact and things like that. But I want to reiterate again that we think a ban is necessary because safeguards aren't sufficient protection.

TALIA KAMRAN: And if I could just add on the issue of a ban in the context of the criminal legal system. A person, a police officer who identifies someone can be, you know, cross-examined, asked why they made the identification that they did. A facial recognition tool cannot be in the adversarial system of our criminal system that is core to our constitutional protections. So, there's not really a way to regulate that to be better. It just simply doesn't fit within the constitutional bounds of the way that we are supposed to prosecute people.

COUNCIL MEMBER HANIF: Thank you for testifying.

I'd like to understand the long-term risks and harms for New Yorkers whose data is breached, and also if you know of other cities that have implemented a full ban or a partial ban on biometric technology facial recognition.

LAURA MORAFF: Sure. So, I can start with the long-term consequences. As has been mentioned here today, biometric information is often unchangeable. Once your biometric data has been collected, there's not much you can do. In a lot of cases, nothing you can do. And so by letting this technology proliferate in the city, we are really creating a state that's impossible to walk back. Companies, residences, NYPD, once they have this information, it can be used against us forever. And things that we might not feel particularly nervous about being recorded today, tomorrow might be criminal. And I think especially in this moment, as the federal government is also ramping up its biometric surveillance efforts, it's really more important than ever that local governments work to protect their residents' biometric data. And so the timing, I think, to this session, we're really hoping that these will move and pass and that we can get that government ban introduced and address this now.

NINA LASHKAJIAN: Yeah. And to the last part of your question, other cities have appreciated the risks, and cities like Boston, San Francisco, Portland, they've banned the use of biometric surveillance. And I think the example Laura gave in her testimony of Legal Aid's client, Mr. Williams, who was arrested, I think that really highlights the harmful consequences of technology like this. And while that played out in the criminal legal system, it's easy to see how a store using facial recognition, calling up the police, leading to a wrongful arrest, will have the same consequence. And that, like she said, can lead to someone losing their job, facing scrutiny from members of their community for having been arrested, all of that. And those harmful consequences can really stay with you for years.

COUNCIL MEMBER HANIF: One more question. For industry groups that support this kind of technology and are saying they feel safer, their customers feel safer, how would you respond?

LAURA MORAFF: Sure. I can start. So, I think we have to consider who feels safer. A company sort of broadly saying that people feel safer isn't going to account for the people who have been falsely flagged by this technology, the people who have been arrested in front of their children, in front of their families, in front of their neighbors, and then again suffer these consequences for the rest of their lives. And I think these bills don't touch traditional surveillance, which our organizations all have our own views on, but this is really about permitting this technology that we know is flawed, that we know is biased, that we've seen time and time again misidentify people with really catastrophic consequences. What we're saying is that we can't use that across the city in places of public accommodation where people are going to buy groceries and diapers, in residential buildings where people are supposed to be able to go home and where their privacy is supposed to be at their pinnacle. What we're saying is these incredibly intrusive and novel technologies shouldn't invade those spaces.

NINA LASHKAJIAN: Yeah. In addition to the very important question of who feels safer, I think it's also what does it mean to feel safe. I think there's a lot of kind of under the surface to some people invisible risks that are posed by this technology. Like if our biometric data is being stored by landlords, by businesses, that exposes us to lots of cybersecurity risks. That is not making us safer. It's actively making us less safe. And in addition, what we've all elaborated on is the risk of harassment and government harm from this technology being in use. And, yeah, just like Laura said, this does not prevent traditional surveillance. I really appreciated that Chair De La Rosa, you started the Committee with emphasizing that though this technology has already started to be in use for years, we haven't seen improvement in retail theft. I mean, that's like one specific example in catching retail theft, and so I think that is just emblematic of the meaning of what it means to make our city safer.

CHAIRPERSON DE LA ROSA: Thank you all so much for coming and for providing your testimony.

The next panel is Jake Parker and Robert Tappan.

You may start whenever you're ready.

JAKE PARKER: Hi, Chair De La Rosa and Members of the Committee. I'm Jake Parker with the Security Industry Association, which is a non-profit representing more than 80 companies headquartered in New York and 1,600 nationwide. Among them are leading providers of biometric technologies using identity access and security products. We're concerned about both of the proposals that the Committee is considering. They would simply outlaw most biometric technologies, despite the protections that are already found in the City's existing biometric identifiers and tenant data privacy laws. This government overreach would intrude into people's daily lives by eliminating their choice to use more secure and convenient services and dictating to New Yorkers how they can and can't protect themselves and their property, making them less safe. The ban in 213 is so broad it would even prohibit biometric authentication to apps on the consumer's own device. Also impacted would be applications for secure account access, payment options, building access, fast lane access to sporting events and other entertainment venues, and security system technology that has been embraced by retailers across the state in the city and a key tool in fighting organized retail crime and protecting their customers and workers from violence. In fact, retail crime is down according to City's own data over the last two years, and even though it remains higher than pre-pandemic levels, it is still reduced. And because use is so common throughout the city, businesses are sure to be caught unaware and subject to litigation. We know that many cases will be frivolous because that's what we've seen so far in cases filed under the biometric identifiers law.

So, turning to 428, this ban denies residents the choice to use biometric technologies for faster and more convenient access to their buildings, and there's really few things that are more important than the security of a person's home, but people do lose their fobs and keys, especially children coming home from school when parents are still at work. Making sure they have an alternative way to get to a safe space is what the Council should be concerned with. Should there be consent and reasonable limitations? Yes, and that's exactly what the current tenant data privacy law requires, but an outright ban stops families from knowing their loved ones have a good way to get into their own home when the inevitable happens and people lose their keys.

Proposals are also based on misconceptions about the security biometric data. It's important to note here that this data is created and readable only within the specific proprietary software used, which is matched based on similarity between saved and comparison information within that system. It is irreversible and it is unusable by third parties and other systems. This is a type of natural cryptography in addition to the actual cryptography that's used, which makes it far more secure than passwords and other information that can be exported by identity thieves and cyber attackers, and there's also the long outdated notion that facial recognition technology specifically is plagued by race and gender bias. U.S. government testing confirms the leading technologies are over 99 percent accurate overall and across more than 70 different demographic (TIMER CHIME) variables. For these reasons, we urge you not to support these measures and happy to answer any questions.

CHAIRPERSON DE LA ROSA: Thank you.

ROBERT TAPPAN: Good morning, Chair De La Rosa and Members of the City Council Technology Committee. My name is Robert Tappan and I'm the Executive Director of the International Biometrics and Identity Association. We're based in Washington, D.C., and I thank you for your forbearance. We arrived at the hearing a little, a lot late, and I do thank you for your understanding.

I'm here today representing the biometrics and identity technology industry on behalf of many of their customers and end users who live and work here in New York City, small business owners, hotel operators, retail stores, apartment building owners and residents, including seniors who rely on biometric recognition technology every single day to protect their lives, their finances, their livelihoods, and their property, as well as to protect those communities in New York City in which they live, shop, work, and serve. We urge Council Members to oppose Intro. 213 and Intro. 428, whether it's a corner bodega in the Bronx, a jewelry store in Queens, or a hotel or restaurant in Midtown Manhattan and in Brooklyn and Staten Island. Facial recognition is not a luxury. It is a frontline defense against shoplifting, fraud, trespassing, and violent crime. These businesses and establishments have been victimized repeatedly, often by repeat defenders who do so blatantly and brazenly. Biometric tools allow owners to identify known bad actors before they strike again. Intro. 213 would strip that protection entirely, banning identification technology at the very places most vulnerable to repeated theft and assault. Intro. 428 poses an equally serious threat to the safety of New Yorkers at home. For seniors living alone in residential buildings or in assisted care facilities, for families in neighborhoods with histories of break-ins and other crime, or neighborhoods with street corners that suffer from drug dealing and gang activity, biometrics and identity technologies provide peace of mind even when a key is lost or a fob is stolen. These systems reassure a tenant, store owner, or an individual that the person who just walked through their lobby or their shop is exactly who they say they are. Banning that technology doesn't make buildings safer or more secure. On the other hand, or conversely, it makes them more vulnerable. We understand the Council and citizens' concerns about privacy, and we take those concerns very seriously, but these bills do not regulate biometric technology. They attempt to eliminate it entirely. That is not a balanced or wise approach. It forces small business owners and property managers to choose between (TIMER CHIME) compliance with the law and physical safety of their customers, employees, and tenants, along with the threat of property or inventory loss. We urge respectfully that this Committee and the City Council reject these two proposals. Thank you.

CHAIRPERSON DE LA ROSA: Thank you.

I do have a few questions. Can you speak to the systems that you both represent? Are they using real-time facial recognition, or does it simply match images against an existing database?

JAKE PARKER: It really depends on the type of application that you're addressing. There's a wide variety of different ways this technology can be used. Fundamentally, it's face-matching software, so it matches images. This could be done for a variety of different purposes. It could be done just to verify that the account owner is who they say they are and that they're attempting to access, or it could be to match against a group of other images to determine if there's a match or not. It really depends on what the application is.

CHAIRPERSON DE LA ROSA: What happens when there is a match? What's the next step? Does a security officer then approach the individual? If there's an error, how does a person rectify it? What are the next steps after someone's been matched?

ROBERT TAPPAN: Chair De La Rosa, I would just say that, first of all, every enterprise, every government office that utilizes these technologies has a different policy. That's probably one of the reasons why you had your colleagues from HPD and OTI. Having those different procedures creates a challenge, a real challenge, and so I can't answer that unequivocally or across the board.

CHAIRPERSON DE LA ROSA: I think that that's what we're trying to solve for here. As you very well testified, you can't neither confirm that a corporation, landlord, business is using the technology responsibly or not. In cases, we just heard the panel before you, which were our public defenders, where Black folks are being disproportionately targeted by this facial recognition technology that has a bias in it, then what is the remedy for the prejudice?

JAKE PARKER: First of all, these bills only address business use of the technology, private sector use, doesn't address law enforcement or government use, so that's not what we're talking about here.

CHAIRPERSON DE LA ROSA: No. I mean, actually, it does because if someone is stopped at Wegmans, for example, and they're arrested for shoplifting because I look like my cousin, there's still a process, a criminal legal system process that happens after that, so there's not a disconnect between what government is doing or what the private sector is doing and what the criminal legal system then does. So, my question to you is very direct. What happens in the case where there is prejudice and the prejudice has been documented for people of color?

JAKE PARKER: Well, so taking the example you just gave, so retailers always have long had programs in place to address organized crime and organized retail theft. Those have often involved keeping track of repeat offenders and also other individuals that have caused maybe violent incidents on their premises. You know, years ago, they might have had a photo book for their staff as they're watching people come in to flag that maybe this person needs to be questioned or approached, and so with modern technology that just enables them to get a technological aid there to flag individuals, and if you're not on some kind of list like that, there's no way a business can identify you. This is only to address those particular individuals, and so what will happen is you typically, a person would be approached for greater customer service. You know, if someone's there to, you know, steal something or do something worse, that's obviously going to deter them, and so that's usually what happens. It most often doesn't involve a call to authorities, and that's where they've been really successful with it.

ROBERT TAPPAN: Right. And I also think that the technology aspersions have been cast upon it about its having an inherent bias or charges of bias in one form or another are founded on old news reports that, you know, stem from a NIST report, National Institute of Standards and Technology, where some of the competitors on accuracy, the companies that were vetting their technology, failed or got poor marks in terms of discerning between different races and color variations of people's skins. We're 10 years hence, at least, from those flawed tests and actors who submitted their technology. The technology has advanced at rapid speed the same way that AI is progressing, so the accuracy rate for most of these biometric technologies, and I'm talking about the major ones, the ones that are done by the larger, more substantial companies that are selling these products and are providing them to law enforcement and to the enterprise, are in the high 90s in terms of accuracy, no matter what. It doesn't matter what color, race, gender, etc.

CHAIRPERSON DE LA ROSA: Well, you know, I appreciate that technology is evolving because technology is ever-changing and ever-evolving, but, you know, just again to point to the panel right before you, the cases they're talking about are not from 10 years ago. There's an eight-month pregnant Black woman sitting in a prison cell because she was misidentified by this information. These are real-life data for a real person who has real consequences, sometimes deadly consequences for some of our communities, and so, you know, I think that that's a huge risk to take and to say that, you know, the technology is evolving and the testing is evolving and therefore we should take that risk. I think that is not government overreach. I think that government has a responsibility to the civil rights of people in order to make sure that communities are safe, and when we say communities are safe, it's all communities, like the bodegas in the Bronx that you talked about and the people that live around those bodegas and, you know, the communities in Queens that you cited. All of us deserve to be safe, and if there's a bias in the technology, then it's difficult to do that.

I want to ask you about, so, you know, we have some data. Our wonderful staff at the Council brought us some data about shoplifting statistics from 2006 through 2024, and it seems that the data that we have, the numbers are not meaningfully declining over the years despite the implementation of facial recognition technology, with the exception of 2020 due to lockdowns and a small decrease in 2023. How do you explain then, you know, despite all this technology being available, we're still, you know, constantly legislating and constantly trying to find ways to prevent retail theft? If the technology is so accurate, right, why isn't it stopping the theft?

ROBERT TAPPAN: Well, number one, it's a deterrent, first and foremost. If people know that they can be identified through this technology, that might be a disincentive for them to shoplift or to go to that place of business to do that, so the correlation between the data you cite and the actual real-life instances of these things may be very disparate.

CHAIRPERSON DE LA ROSA: So, 2006, according to our data, there were 16,983 instances of shoplifting. 2025, 50,000. So, it's gone up exponentially, and the data's there, and the data's gotten better since 2006.

JAKE PARKER: If I could, you know, I don't have the same data in front of me that you have, but I definitely looked at the City's data last night. Between 2024 and 2025, there was a 15 percent reduction in retail theft. But looking over a longer period of time, obviously that could be different, but as Robert said, it's hard to measure. You can't measure what didn't happen, right, so the deterrent effect, it's notoriously hard to measure, but this technology is being adopted by retailers throughout the city very enthusiastically. They must be seeing some kind of value there, otherwise it would be making an investment.

ROBERT TAPPAN: Right. And another important data point is also the economy. Retail crime, other crimes sort of correlate with the, you know, tough times and more flush times, if you will. So, you know, there are other vectors and other factors that need to go into just that raw data of numbers of shoplifters or crimes committed.

CHAIRPERSON DE LA ROSA: When your system identifies an individual, what additional information is available to you? For example, do you see whether a person has a criminal background, their name, or other identifying information? In general, I know every situation is different, every technology is different, but in general, are you seeing a profile on a person, or is it just their face and their name?

JAKE PARKER: All the technology can do is match images, so if you have other information about, you know, a person, they would come from other sources.

ROBERT TAPPAN: Right.

JAKE PARKER: It's all it does is match images.

ROBERT TAPPAN: Another thing, too, there are a couple of different approaches on the biometric measurement. Number one is there's one-to-one, and that's when you use your face to open your iPhone, right? Also, too, in my own personal case, and I've testified before the City Council now, this is my third time, both Jake and I testified 2023, 2024, and now, and I've used this story before. My mother suffers from dementia. She's in an assisted care facility that has a secure building. When I go in, I've already registered my face, my driver's license, my phone number, and it goes into a facial recognition system, and when it accepts it, I get the same sort of sticker I got when I, yeah, right? So that allows me in. I don't want people to willy-nilly be able to come into a facility like that and cause harm to any of those people, most of all my mother, so it's those sorts of things. That's one-to-one. It's checking to see whether your credential matches your face.

And then, in the case of, let's say, TSA security at the airport, that's one-to-many. That's a database that your driver's license and your face, it verifies the credential, and then, if you happen to be on a watch list or have some sort of travel-related or airport-related violations, then that flags that.

CHAIRPERSON DE LA ROSA: Which this bill doesn't speak to airport lists. But, you know, I want to recognize that, yes, there are instances like when you walk into this building or you walk into a government building where you're, obviously, there's a badge that's produced and there's security measures being taken. That's completely different from a Rite Aid or Wegmans, a private company, using data to basically make a prejudice of a profile of a person. And let me just say that people can commit crimes and they still need to go to the pharmacy and get medicine. They still need to go buy toilet paper.

They still need to buy water. And so, like, I can't really justify the use of this technology that is going to have a prejudice on that specific person for getting their toiletries, for getting their groceries. Like, everyone still has to eat. Everyone still has to use the bathroom. Everyone still needs medicine. Versus if they're coming into a government building or whatever, we expect for there to be security measures taken. So, it's a different, like, it's not apples to oranges, you know, in the case of your mother, which I'm sorry that she's going through that, and I know that can be extremely difficult. For the protection of the folks in that assisted care facility, it makes sense. They're a vulnerable population that they would have security measures. But if you were charged with a crime or had a past criminal record, that's still your mother. You still have the right to go see her.

ROBERT TAPPAN: Right. But that one-to-one just matches my credential, my driver's license.

CHAIRPERSON DE LA ROSA: I get it.

ROBERT TAPPAN: And so, it doesn't go to…

CHAIRPERSON DE LA ROSA: But the risk is that other category of information that we do not know if all of the companies that you all represent or that, you know, are using this technology are checking up against, right, to ban people from establishments, to make assumptions about a person's behavior based on who they are, what past history they may have, you know. I mean, imagine if we all got, you know, prohibited from coming into this building because we have parking tickets. This would be an empty hearing.

ROBERT TAPPAN: But also, and not to belabor this point, but, you know, in places like restaurants and bars, especially in communities where, and I'm not talking about New York per se, but I'm sure it happens here as well. If there is someone who comes in who is a constant, you know, starter of fights or after he or she has won too many, becomes belligerent and wrecks it for the other customers, you know, maybe there's a bouncer that knows that person's face. But if that person is arrested for something like that, then they can be on a watch list for just that particular bar. And it's not about their criminal record. It's about this is a person that we don't want in our facility. And I would guarantee you that if I had committed some crime or was wanted, if I was coming downstairs and I gave my driver's license, it very well may flag something that would prevent me from testifying before you.

CHAIRPERSON DE LA ROSA: I mean, I don't think we do that here because we are, you know, public open meetings law allows anyone to come in.

ROBERT TAPPAN: But my driver's license was scanned as was everybody else's.

CHAIRPERSON DE LA ROSA: Yeah. Of course. But again, there's a different dynamic when you're talking about a government building and you're talking about going to Rite Aid. You know what I'm saying? It's not apples to apples. But let's agree that we both have a disagreement in how far the technology should go.

I want to pass it to Shahana, to Council Member Hanif, to ask a few questions.

COUNCIL MEMBER HANIF: Thank you.

So, this is a question for Jake. You mentioned in your testimony that there are common misconceptions based largely on Hollywood portrayals and inaccurate media narratives of biometrics. Could you just go into that a bit more?

JAKE PARKER: Well, as I explained earlier, I think there's a misconception about the security of the data that's created. It's within each software.

COUNCIL MEMBER HANIF: But could you give me an example?

JAKE PARKER: So, like if, say, my image…

COUNCIL MEMBER HANIF: No. An example from a Hollywood portrayal or an inaccurate media narrative. Not a hypothetical, something that has been out there that has been inaccurate.

JAKE PARKER: The idea that you've seen in movies where a system like this would be able to take someone's image and then pull up vast amounts of data, a profile on someone, which is definitely Hollywood portrayal.

COUNCIL MEMBER HANIF: It's pretty scary. It's like blackmail.

JAKE PARKER: But that's not the way it works in real life. So, there's not a connection.

COUNCIL MEMBER HANIF: Pretty scary.

JAKE PARKER: So, a system using retail security, it's not connected to someone's criminal records or vast amounts of information on them. It's only about their history in that particular place. These are typically very small watch lists.

COUNCIL MEMBER HANIF: Well, I'd love to get a full list of the movies or shows you're providing examples for here.

Do you believe that biometrics should be used as an intelligence tool to target immigrants, as our federal government is doing right now?

JAKE PARKER: I think that there's laws and regulations around all these technologies need to be followed very closely.

COUNCIL MEMBER HANIF: Which law?

JAKE PARKER: I mean, we're here talking about business uses of the technology.

COUNCIL MEMBER HANIF: Could you describe which law? Even though we're talking specifically about businesses of public accommodation and residential buildings, it is important to know that the companies you all represent, they are operating in a variety of sectors. And so one use doesn't prevent another sector to go without it being used.

ROBERT TAPPAN: Well, you're right in making that statement. But at the same time, there's also other things that are not necessarily 100 percent biometric related. Like your phone. Your phone is…

COUNCIL MEMBER HANIF: Robert, I only want to know if it should be used as an intelligence tool, which it is being used as right now.

ROBERT TAPPAN: Well, it depends on…

COUNCIL MEMBER HANIF: You can just say you don't have an opinion on that.

ROBERT TAPPAN: I will tell you that retail stores are not using it for intelligence.

COUNCIL MEMBER HANIF: That wasn't the question.

ROBERT TAPPAN: Yeah.

COUNCIL MEMBER HANIF: That wasn't the question. So, do you believe that biometrics should be permitted without any regulations or consent-based? The example you gave, Robert, there could be other members of the facility visiting who opt out. What's your take on the opportunity to opt in or opt out?

ROBERT TAPPAN: Absolutely. I mean, at our Association, we have a white paper on ethical use of biometric technology, and the first point is respecting the person and related data. Second, upholding a commitment to transparency. Communicating with data subjects about what biometric information is being collected, what it will be used for, to whom it will be shared, and for how long it'll be retained. Third, working to secure biometric data to minimize it. Biometric data, unlike one of the colleagues from the previous panel had averred, is that biometric information, for the most part, is not able to be reverse-engineered. It's encrypted. So, so-called leaks of biometric information, there may be leaks of files, but there aren't necessarily leaks of biometric information across the board there. And of what use is it? Biometrics are individual to the person because of their characteristics, and…

COUNCIL MEMBER HANIF: I think we understand the definition here.

ROBERT TAPPAN: Right.

COUNCIL MEMBER HANIF: Do you sell or share the data that's collected among the groups that you represent?

ROBERT TAPPAN: To my knowledge, our members don't.

JAKE PARKER: Well, I mean, as Robert explained, there's no… the data is not usable outside the system that created it. So, there's no… it would be… if it is extracted somehow, it'd be completely useless to anyone so.

COUNCIL MEMBER HANIF: And then you're okay with biometric tools that are the same, of the same standard, at a Bronx bodega and at the airport for TSA check-in?

JAKE PARKER: People should be using the most accurate technology available so…

COUNCIL MEMBER HANIF: So, you're saying those two technologies could be, potentially, the same kind of tool?

JAKE PARKER: The software, it's the matching software. It could be used on a phone to match your photo to your enrollment image, or it could be used to compare against a list of people who are boarding an aircraft in a day. That core function is the same.

ROBERT TAPPAN: But, you know, the bodega owner is not buying what TSA has. I mean, these are…

COUNCIL MEMBER HANIF: That's exactly what I wanted to know.

ROBERT TAPPAN: It's not as robust, and it's usually localized. It's catching repeat offenders or the images of people who have previously committed crimes in that bodega or in that neighborhood.

COUNCIL MEMBER HANIF: And then outside of just providing the technology, is there an evaluation that's done annually or quarterly to assess, this tool helped us prevent theft all across New York City, or is there an evaluation process, or are you just providing the tool and the technical support on how to use it?

JAKE PARKER: So, you know, I've heard examples of retailers, once they implement the technology and have the right set of processes around it, they're reducing their theft by like 80, 90 percent in some cases. So that's anecdotal.

COUNCIL MEMBER HANIF: We're here to really understand your sector.

ROBERT TAPPAN: Right.

COUNCIL MEMBER HANIF: And I would love if there's a possibility of us being able to visit a vendor that has had that kind of success.

ROBERT TAPPAN: Sure, absolutely. I'd be happy to set something up with one of our vendors.

COUNCIL MEMBER HANIF: That would be great.

ROBERT TAPPAN: Yeah. Also too, and I didn't go through all the points, and I won't belabor this, but there are two additional points in this ethical standards white paper is promoting accountability. So, that is constant training of people, limiting the use to people who are privy to this information. So, it's limited to security people and let's say senior executives, if the case is significant enough. So, there are safeguards put in place already that these companies want their customers to adhere to. And then also to resolving any cases of redress, which goes to if someone believes that they have been wrongly identified or if they've had some sort of accusation that has been made against them that biometric information has provided a foundation for that case, then there should be a process for them to be able to seek redress in the same way that people recover their credit and other ways of rehabilitating the record or correcting the record.

COUNCIL MEMBER HANIF: So, you're saying the folks at Rite Aid who were wrongfully charged that they can participate in an appeals process to ensure their safety moving forward.

ROBERT TAPPAN: I don't know the specifics of the Rite Aid case, and I'm sure it was egregious.

COUNCIL MEMBER HANIF: I mean, what I'm trying to get at is that if one of these tools could aid Rite Aid or any other chain to wrongfully charge folks and, honestly, it's like it's financially draining, it's socially draining, and you're traumatized from having your entire data not only used, but also now charged with something that you have not done. So, I'm just trying to understand like what do you say of that?

ROBERT TAPPAN: Well, I think the scenario that you describe is a little conflated and inflated because in the case of, if you set side by side, if you have biometric technology identifying someone who has been accused of, let's say shoplifting, there is a video record and then there is a identification record if that person is apprehended, right? How much different is it when a security guard sees someone and goes, I just saw that person steal something. How do you measure those two? One is much more accurate, and one is relying on just human judgment. And those two things are apples and oranges. Biometrics are much more accurate. But no technology is 100 percent correct all the time. And that's why innovation exists so.

CHAIRPERSON DE LA ROSA: In that example though, our public defender friends gave us this language, right, so if that were to occur and there was a criminal trial, that bouncer, security guard, police officer would come in, testify, present their evidence. Someone could question them. Someone could present. We can't do that with technology. We can't question bias. We can't question motivation. We can't question details. We just have to kind of take it at face value. So, the accountability is different when it's a human being. It could be human error. We could get to that through questioning versus a technology that we can't question.

ROBERT TAPPAN: But you can play the videotape and you can also show some of the information that's been collected and see that there's a match or not so.

JAKE PARKER: I mean, there's an assumption there that the action taken, someone being arrested and charged is based only on some kind of flag like that. I don't think that's reality. You're going to have a lot of other factors at play there. It's not going to be the reason why those things happen.

CHAIRPERSON DE LA ROSA: I wanted to ask about, so going back to the bodega example. So, if I have a bodega and I contract the technology and one of your company services, they create a profile based on the people that come into my bodega. So, if Mr. Williams comes into my bodega on Tuesdays and then Mr. Williams visits another bodega down the street, is that information shared with the bodegas in the neighborhood?

ROBERT TAPPAN: There is not a vast bodega network, I promise you. No. Unless the bodegas are owned by the same person, I think that would be really the only way that information sharing would be appropriate.

CHAIRPERSON DE LA ROSA: And the profiles and the images that they're comparing from would be based on the people that have walked into that bodega, not like a random database.

ROBERT TAPPAN: Right. Right.

CHAIRPERSON DE LA ROSA: Okay. And what if I have a twin, an evil twin that's just going around stealing Twinkies?

ROBERT TAPPAN: So, Chair De La Rosa, your evil twin has significant differences than you do, even though you may look exactly alike and she is the spitting image of you…

CHAIRPERSON DE LA ROSA: And the technology accounts for that?

ROBERT TAPPAN: The technology in many different ways, but it's the measurement of your face, it is your vein patterns under your skin, your irises are different. Every individual has unique irises in the same way that they have unique fingerprints.

CHAIRPERSON DE LA ROSA: And that information is available because when we ask the question about what profile information pops up and populates, the question was like, it's an image. So, there's not a profile attached to that image. So, is there information about my iris? Is there information about my vein structure? Is there information about my double chin? Like, what information is on there?

ROBERT TAPPAN: No, ma'am. In the case of iris, you have to be, I think there's a range that the camera has to be able to take your, and it's usually opt-in, and so that process is much different. You can't catch irises at a crime. You can catch people and faces at a crime if there's close circuit television or cameras and biometrics, but not with just general facial recognition, as opposed to iris is much more granular and much more focused.

CHAIRPERSON DE LA ROSA: There's a gray area then in the comparing of images versus the information behind the image.

ROBERT TAPPAN: And the different modalities of technologies, like fingerprint, like voice, like facial features or vein print, gait, people walk it very individually. You can measure someone biometrically by their walk, those sorts of things.

CHAIRPERSON DE LA ROSA: Okay.

COUNCIL MEMBER HANIF: Have your clients gone through any audits? Is there an evaluation independently or within the company that takes place?

JAKE PARKER: Well, just in the last one, none of those other biometric technologies we talked about are relevant for retail security, just to make that clear. You know, when we're talking about facial recognition technology, there's an established government program that evaluates the performance of the matching software, but there is also for some other biometric modalities as well. So, the U.S. government is basically the premier source of that information.

ROBERT TAPPAN: Right.

COUNCIL MEMBER HANIF: So, the auditing is taking place by the federal government. Is that what you're saying?

JAKE PARKER: Of the software.

CHAIRPERSON DE LA ROSA: Of the software.

ROBERT TAPPAN: Of the software as it is applied in the U.S. government context.

COUNCIL MEMBER HANIF: Great. Now I like biometrics even more.

And then, you know, the conditions of our Rite-Aids, Duane Reades and Walgreens are terrible because everything is locked up.

ROBERT TAPPAN: Right.

COUNCIL MEMBER HANIF: But do you feel okay going into a locked up Rite-Aid?

ROBERT TAPPAN: I don't like it, but it's a necessity. But that's not because of biometrics. Biometrics would help.

COUNCIL MEMBER HANIF: Well, outside of the biometrics, because we know Rite-Aid certainly was a perpetrator and did a lot of harm. I'm just trying to understand that it is very unusual and very scary to go in, and also I don't want everybody to know what I'm buying. I go in to buy the Trolli gummies. Like you guys don't need to know that.

ROBERT TAPPAN: But Rite-Aid or any other retail store knows what you buy when you use your membership card so there's a full database of, and that's collected because, that's why it sends you targeted ads.

COUNCIL MEMBER HANIF: I'm just trying to make the point that having your shelves locked and having the surveillance technology is creating a space of intensity, anxiety, and also mistrust among people, and I think that we could do better without this kind of technology. Now, my bill does not ban all biometrics, and I think that my bill is quite measured and also it doesn't say you can't use video surveillance. But what we are seeing that is escalating around surveillance and thinking that every other person is a thief is quite, quite scary for New Yorkers.

JAKE PARKER: Could I say something?

ROBERT TAPPAN: Yeah, please.

JAKE PARKER: I think you also have to consider though, what the situation would look like without these advanced tools. So, right now you have stores that are under stress from, you know, from theft. They have to lock things up. But if you didn't have these tools, they may not be there at all. So, we have to consider access as a key, you know, objective here.

COUNCIL MEMBER HANIF: So, you think if the Rite-Aid isn't locked up, that one could go in and see that the shelves are empty? Is that what you're suggesting?

JAKE PARKER: No. I'm saying it may not make business sense for that business to actually have that location open at a certain point.

COUNCIL MEMBER HANIF: These are chains though. We're not talking about.

ROBERT TAPPAN: Yeah, but we, in New York City…

COUNCIL MEMBER HANIF: But I'm just trying to…

ROBERT TAPPAN: Yes, ma'am. We're having a spirited discussion here.

COUNCIL MEMBER HANIF: Yeah.

ROBERT TAPPAN: You're making very, very valid points, but you're asking us questions, and I'd like to be able to provide at least my version of the answer for you. And, you know, biometrics is not the reason that these goods are behind shelves. Crime is the reason. And in order to combat crime, and especially rampant crime when you have, you know, gangs of people going in and just, you know, filling up trash bags and leaving, there has to be some sort of safety.

COUNCIL MEMBER HANIF: Where has that taken place?

ROBERT TAPPAN: All over the country.

COUNCIL MEMBER HANIF: But we're in New York City. We're talking about…

ROBERT TAPPAN: It happens at Gucci.

COUNCIL MEMBER HANIF: We're talking… the example was Rite Aid.

ROBERT TAPPAN: Okay.

COUNCIL MEMBER HANIF: Right. It's primarily food…

ROBERT TAPPAN: They're stores, they're retail stores.

COUNCIL MEMBER HANIF: Drugs, and household items. That's not a great comparison, but I'll move on and pass it to the Chair.

CHAIRPERSON DE LA ROSA: Yeah. I just want to say, like, I get that, and it may be happening at, at a scale, but biometrics is not stopping a person from walking out of a grocery store with a bag full of stuff. Like, a security guard will, or there's other ways to do it. I understand the deterrence as a mechanism, but I don't think it's the only way.

But I digress, because we still have a lot of panels to go.

I want to thank you all for your time and for submitting the testimony. The Committee will continue to look at this and continue this discussion internally.

ROBERT TAPPAN: Thank you so much.

CHAIRPERSON DE LA ROSA: Thank you so much.

Up next, I want to call up Cynthia Conti-Cook, Shruthi Velidi. Sorry for the names. Please just come up and correct it on the record, Sergio De La Peña, Medha Raman, and Corinne Worthington. And I think there should be five chairs there.

Whenever you're ready, at either side of the table is fine. Thank you.

SHRUTHI VELIDI: Thank you, Chair, for the opportunity to testify today. My name is Shruthi Velidi, and on behalf of New York City's chapter of the Democrat Socialist of America's Tech Action Working Group, we support the passing of Bill 0213. DSA has over 14,000 members in New York City and over 100,000 members across the nation.

We are facing an unprecedented expansion of mass surveillance. In 2025 alone, 58 percent of ICE arrests in New York City involved individuals with no criminal convictions or pending charges. Immigration enforcement today relies not only on government authority, but also on private technologies, including facial recognition tools, biometric databases, and large-scale data-sharing agreements between corporations, data brokers, and government. Data collection has no boundary. Information can be repurposed beyond its original intent, and privacy is optional rather than protected. New Yorkers should not be forced to accept biometric surveillance as part of simple daily activities such as buying groceries or going to a concert. Introduction 0213 grants people the power to exercise their rights when it comes to biometric surveillance tracking while simultaneously preventing any place or provider of public accommodation from refusing service, charging different prices or rates, or otherwise penalizing customers who do choose to exercise their rights. We also support the strong provisions in the bill that prevent the disclosing, selling, leasing, trading, or sharing of biometric data in exchange for anything of value with any third party.

Biometric technologies are often framed as innovative, efficient, more accurate, but this is far from the truth. In reality, these types of tools are immense privacy and security risks and disproportionately harm marginalized New Yorkers. However, while we support the passing of this bill, we recommend addressing two key gaps in the existing text. First, accessible and informed consent must be clearly defined. The bill calls for disclosure of data collection via signage in plain, simple language. However, this does not cover people with visual impairments, nor does it account for non-English speakers or minors who cannot consent. Beyond accessibility of notice, the bill also fails to establish the substantive conditions necessary for informed and meaningful consent. The proposed language also neglects to require detailed notice specifying what data is collected and for what purpose. Additionally, when under-specified, written consent can be an ineffective consent mechanism depending on how it is presented. For example, research has shown that dark patterns, for example, in online cookie notice and consent procedures effectively manipulate people into consenting. Similarly, consent buried within broad terms of service or loyalty program agreements may technically satisfy the requirements in the bill without customers ever meaningfully registering what they have agreed to. We recommend implementing a more meaningful approach to consent, prohibiting dark patterns where individuals have to opt-in affirmatively with full knowledge of what they are consenting to (TIMER CHIME) receive notice as to how the data will be used, how long the consent is valid for, accessible in multiple languages, and with the option to revoke or revisit that consent at any time. Addressing these gaps would make the consent more accessible and meaningful. Thank you for the opportunity.

CHAIRPERSON DE LA ROSA: Thank you.

MEDHA RAMAN: Good morning, Chair De La Rosa and Members of the Committee. My name is Medha Raman, and I'm testifying on behalf of the New York Civil Liberties Union in support of Intros 213 and 428.

The growing prevalence of biometric surveillance technology by landlords and in places of public accommodations poses a danger to all New Yorker civil liberties. Biometric surveillance technologies enable invasive tracking of people's identities, movements, and associations, threatening their rights to privacy and equal treatment under the law. Facial recognition and other forms of biometric surveillance technology are also highly flawed and racially biased, as demonstrated by numerous studies and some individual testimonies, including those we've heard today. In the residential context, where Fourth Amendment protections are at their strongest, tenants should not have to live in fear that their landlords are tracking their comings and goings and gathering biometric data on them and their guests. This data can then be used to evict rent-controlled tenants for minor policy violations or share with immigration enforcement. Similarly, when stores such as Wegmans, Whole Foods, Macy's, and Fairway track shoppers and gather their biometric data without their consent, the consequences are significant. As Council Member Hanif highlighted earlier, in 2023, the FTC banned Rite Aid from using facial recognition surveillance for five years after their technology misidentified thousands of customers, disproportionately people of color and women, as previous shoplifters. Suspected individuals were then followed around the stores and searched, ordered to leave, or publicly accused of shoplifting. Other businesses may also use this information to implement surveillance pricing, identifying individuals to change prices dynamically based on their characteristics or perceived willingness to pay.

Without stronger protections, unrestricted use of biometric recognition technology risks creating a constant state of surveillance, wrongly excluding people from public life or their homes due to misidentification, and further exposing communities of color and immigrants to potentially dangerous interactions with law and immigration enforcement. To urge that the proposed legislation can fully address these issues, we urge the Committee to consider the amendments fully detailed in our written testimony. The NYCLU thanks the Committee for the opportunity to provide testimony today and for recognizing the need for stronger protections against biometric surveillance. We urge the Committee to pass Intros 213 and 428 and to go a step further by also prohibiting biometric surveillance in other areas where critical rights are at stake, notably law enforcement and government use. Thank you.

CYNTHIA CONTI-COOK: Good afternoon. My name is Cynthia Conti-Cook. I'm the Director of Research and Policy at the Collaborative Research Center for Resilience. Thank you so much for holding this hearing.

At the Collaborative Research Center for Resilience, we ensure government use of technology does not undermine democracy. We investigate incoming government technology and digital public infrastructure, and we do investigations that help communities meaningfully participate in government use of technology and understanding it. We understand the harm that individuals face as a result of surveillance policing as not just a harm to individuals, but harms to entire communities. And when people are given the rights to access freedom or access facial recognition technology as the previous panel, for example, proposed, it doesn't just impact their individual rights. It impacts their entire community's rights, and it's from that lens that I really want to ground this testimony. I was previously a civil rights attorney and investigated municipal liability claims for many, many years. And I think a lot about how patterns and policies and practices through the use of government technology not only implicates and harms the people who are subjected to it, but it creates liability for the whole city that taxpayers are going to have to hold the check for. And that is on top of the harm that

New York City communities are going to experience. They also have to pay for the lawsuits that will come from any municipal liability found to have a pattern, policy, or practice of the type of discrimination, of the type of bias that you all are very honed in on and correctly concerned about. In addition to that, we are also the taxpayers that are paying them, because they are often vendors, and so we can see how we are paying three times for these services. There's well-publicized problems. The previous panels mentioned them all about surveillance policing. It is very concerning. And I just want to mention that despite what the previous panel said, Home Depot has absolutely shared facial recognition data with immigration law enforcement. We know that from news reports.

I also want to think and propose testimony about what Council Member Hanif, you said earlier about where is this going, not just where are we already. And where this is going is not just surveillance policing, but surveillance pricing. And we know that the Wegmans and the Rite Aid and the many stores that are, for now, talking about safety and security and the need for biometric technologies for the purposes of probably also getting a discounted insurance policy, that they're also thinking about the potential to use surveillance pricing to be able to look at Mr. Williams coming to the bodega for the fourth time this week and know that we're going to maybe mark up a little bit on the margins for how much he's going to spend on whatever it is he commonly buys so the collection of biometrics (TIMER CHIME) Thank you. Just to name… the collection of biometrics itself and not just the deployment of facial recognition is what I would really like to see more expansion in these bills around and an understanding that biometrics is a critical component and enables a lot of other technology, including digital identity, digital wallets, online verification, as well as agentic AI, which looking around the corner, there's a lot of reasons to pause on all of those things, seeing the chaos and the potential harm that all of those technologies combined could cause our communities. Thank you.

SERGIO DE LA PEÑA: Thank you, Chair De La Rosa and this Committee for this crucial hearing. I am Sergio De La Peña. I'm the Legal Director of New

York County Defender Services, a public defender office here in Manhattan for decades.

So, we will submit later today some written testimony taken from the vantage point of our clients and what they've experienced in reaction to a lot of these technologies that are being discussed today. But I want to, in these moments, take a more kind of fundamental view of all of this. We do support and applaud these two pieces of legislation. We just say keep them coming. More. And the reason I say that is because I think even though it's only March, I want to nominate this as the scariest hearing of the year. Because we're not talking about a hypothetical future, dystopian surveillance state. We're living in it. We're living in it. And so the question becomes, I'm old enough to remember when there was such a thing as privacy, when some people felt more private than others, what they were comfortable sharing. And that was considered a kind of inalienable right of every individual to decide how much of their information should be known by others. Today, I'm realizing that probably the last time I went on an investigation, potentially my gait was monitored, recorded, and kept for who knows how long, used for who knows what purpose. I will say that I'm glad the Office of Technology and Innovation sent the representative today. They didn't really allay any of my fears. And you asked them, you know, what agencies use these things? And he said, I don't know. Somebody brought up the MTA using facial recognition for the untold millions of people who use our subway system. They say the MTA doesn't have to report to us. The MTA doesn't have to report to them when asked about vendors. There was a lot of I don't know. So, it appears that in the public sphere, certainly the oversight isn't particularly robust. And hopefully that's about to change. But that's the public sphere. In the private sphere, it's clear there's absolutely nothing. I believe Public Advocate asked, you know, what's in place to monitor something like Wegmans or Duane Reade or the various commercial entities we've discussed, and it was just birds chirping. There is no oversight. And again, my fears weren't allayed when the latest purveyors of these systems came here to protect their financial interests, although I was gratified to learn that really they're just worried about that 14-year-old girl who lost her key and really needs to get into her apartment. Not any money or the ability to sell us surveillance, deep state technologies that we don't then monitor, that we have no idea how they're used. There was references a lot of present tense. You can't take a face and pull up a whole thing like on that Hollywood blockbuster you saw. You can't do that today. And rest assured, if they're not doing something, it's because they don't have the technology to do it or there's no money to be made. But the collection is happening today. And three years from now, it may very (TIMER CHIME) well be possible to do that Hollywood thriller where you pull up someone's face and tell them what they got in macroeconomics at their state university. So, again, I applaud this hearing. I think the burden of proof is on those who want to continue to bolster our surveillance state. They should have to demonstrate why it's necessary for Duane Reade to collect and monitor my gait when I'm buying deodorant. It should not be the other way around. Thank you.

CORINNE WORTHINGTON: Chair De La Rosa, Council Member Hanif, thank you for the opportunity to testify in support of Intros 213 and 428 today. My name is Corinne Worthington. I'm the Advocacy and

Community Engagement Manager at the Surveillance Technology Oversight Project.

I want to correct something that one of the previous panelists said, which is that studies done by the National Institute of Standards and Technology are showing that these biometric recognition systems are more accurate than ever and that they're 99 percent accurate. That's in laboratory conditions. Studies show that in the wild, and so when you're shopping at the bodega or going to Wegmans, those kinds of conditions, these systems are much less accurate. The National Institute for Standards and Technology stopped tracking what the accuracy was for in the wild conditions in 2023. So, we have no way of knowing from those studies in particular how accurate these systems actually are in practice. Studies done by IPVM and other independent assessors show that they don't live up to these standards.

I also want to just say one other thing. We aren't data subjects. When these systems are misidentifying individuals, it's not just in a theory. It looks like a young woman in the Bronx who was an intern at my organization being stuck outside in the rain because she can't enter her apartment building. It looks like shoppers at Rite Aid being tracked, followed, harassed, ending up on a national database of potential threats to Rite Aid. In a city as diverse as New York, it's unacceptable that landlords and businesses knowingly deploy discriminatory technology. And while the issue of bias can't be understated, it's not the only issue here. And in fact, a system that can identify and track people with 100 percent accuracy unlocks an even bigger and more dystopian problem. The reality is that with the expansion of biometric technology into homes and businesses, New Yorkers can be tracked in all aspects of their lives. This is a particular concern for immigrant New Yorkers, where over the past year, we've seen hundreds of them abducted off the streets and disappeared into the network of ICE detention facilities. We've seen Home Depot and other businesses collaborate with immigration enforcement. And without any oversight, guardrails, or regulations, this will continue. It is past time for New York City to take a stand against this invasive technology. We encourage the City Council to do so now by passing these two Introductions, 213 and 428, and by going further to ban police and other forms of law enforcement and government surveillance technologies. Thank you.

CHAIRPERSON DE LA ROSA: Thank you all for your meaningful testimony. Certainly, want to say that that is the work of the Committee that we're trying to really root in, is like, where do we need to plug the holes that right now exist in the system overall, and I'm looking forward to using our oversight powers to do some of that. Although our jurisdiction is limited, but the platform to talk about these things is not.

I do want to ask a few questions. I believe you testified about consent. Somebody testified about consent. Okay. And you mentioned dark patterns. Can you give us some examples of that?

SHRUTHI VELIDI: Yes. Example. So, I think you find a lot of dark patterns in online cookie notices, especially when folks are using the web. I think a lot of these dark patterns essentially confuse participants or they present them in very complicated or just complicated and non-simple ways. But I'm happy to provide more examples in our written testimony afterwards as well.

CHAIRPERSON DE LA ROSA: And for the entire panel and whoever wants to jump in, can we talk more about what consent could look like? I mean, we can talk about it in terms of like walking into a grocery store or even in government functions. I'd love to talk more about consent.

MEDHA RAMAN: I'll just say one of the goals of these pieces of legislation are to address areas where there is a particular imbalance of power. So, in the landlord-tenant context and in places of public accommodations, it's places that you have to go. They're sort of essential to daily life. And in the law enforcement context as well, these are things that come up regardless of whether you were opting in to being a part of it. So, I think consent in a lot of ways just doesn't go far enough because of that imbalance of power and those issues that we see there.

CYNTHIA CONTI-COOK: I 100 percent agree and would just add, as was previously mentioned, the idea that the burden should shift to the person who then has to understand what it means, what it means for them as an individual, what it means for them in relationship to that store, what it means for their community in relationship to that store. The true ability to have a meaningful and informed consent in that context is very limited.

And the reference to dark patterns really refers to the capacity of people in asymmetrical power dynamics to take advantage of the urgency, whether that's because you need to get into your building in the rain or whether that's because you really need, you know, Lactaid milk for your kid because they have lactose intolerance. Either way, the power structure is taking advantage of something that they know about you and it's giving you a limited choice. And then within that limited choice, whether it's deciding whether or not to go into the most proximate grocery store that has facial recognition and you have to go through this consent structure or whether it's through the building that you want to live in, but it has this, you know, surveillance screen at the front door, it limits your choices to really identify and make the kinds of living decisions you want and also that other people in your community might want you to make on their behalf.

CORINNE WORTHINGTON: I think there's also something to be said for transparency about how this data will be used. I think what Council Member Hanif was saying about allowing your biometrics to be collected to buy specialized running shoes with a hyper-specific purpose and potentially, I would go further to add there should be much more stringent data retention laws around that, about how long companies would be allowed to continue to hold your data before deletion. But that is very different than, you know, signing a contract with your landlord or going to buy groceries, where you don't really know how that technology would potentially be used, stored, how long it would be kept, and it's also an issue of these coercive environments. As others have said, the imbalances of power make it such that informed consent in those environments where you're seeking out something that you need rather than a luxury, something that you want, it's difficult, if not impossible, to maintain non-coercive consent in those scenarios.

CHAIRPERSON DE LA ROSA: Great. I'm actually working on legislation on pricing and AI. Do you want to share more thoughts around that? I know you brought it up in your testimony.

CYNTHIA CONTI-COOK: Oh, 100 percent. I mean, if you go to some of these industry conferences and hear them talk about the future of their technology, it sounds very different than their testimony sounded today. The future of their technology, as they promote it, integrates biometric identification technology with digital identity, with digital wallets, and voila, you can walk into a store, not have to interact with any clerk or any person, and walk out with the product that you wanted and everything is handled by a system of biometric identification that connects you to your ID and then connects to your wallet to verify your purchase, etc. That's how they present the technology when they talk about it at their industry conferences.

Now, what that means for anyone who is, for example, inside the store and unable to get in, what it means for the way that everyone else is treated, if cash is not taken, if there is no clerk, if there isn't someone who can answer a problem, if there isn't someone who can unlock a shelf, people have a hard time navigating these places, often actually limits who can go in. Digital identity has been passing and being implemented all over the world, and in some countries where there's been digital identity implemented, people haven't been able to get into hospitals or haven't been able to get healthcare, and while promoted as easing access and facilitating access, and as being inevitable as it's promoted, it is not often enough talked about in the ways that it as easily excludes people as it makes access easier for some, but certainly not for all.

And as I said earlier, this is not just a safety issue. They talk about it in terms of safety and making the shopping experience more safe and secure for all customers and for all people, but it is not just a safety issue. It is, one, an insurance issue. They have pressure from insurance companies to create data sources that they use for compliance, for audits, to get cheaper insurance, but it's also building up this large surveillance pricing network where, for example, if you needed to, you know, have a certain thing, someone, if your cough was detected by your Alexa at home and then you went to buy a cough suppressant nearby, that that could be ticked up in price for you because that kind of information has been correlated around you. Now, that is still in the future, but it is the kind of concern that we should get ahead of today.

CHAIRPERSON DE LA ROSA: Great. Thank you for elaborating on that.

You want to add, both of you?

SERGIO DE LA PEÑA: I want to reiterate that I think the inflection point is not what they do with the data. It's when they collect it. So, we've seen examples of private entities say, we'll take your DNA to tell you who your great-grandfather was, but then that company goes out of business and sells that to another, and so years pass, but the rules that we set forth today reverberate for decades. And there's things we can't even conceive of right now, and they're banking on that for a commercial motive. So, I think it really is about restricting collection wherever possible. And we're finding out a lot today that that collection's already happening, and it doesn't appear that there was the greatest barrier to that. They just chose one day to start doing that. They chose to purchase the program and start doing it without any real societal kind of affirmation that we're okay with this.

CHAIRPERSON DE LA ROSA: Got it.

CORINNE WORTHINGTON: I also want to highlight a bit about the way these systems are marketed. We've heard a lot of talk about public safety, but in fact, the way that these systems are marketed by the vendors to potential purchasers are, in the context of landlords, they're marketed as a way to evict tenants, potentially. Particularly if those tenants are in rent-stabilized units, so that you can catch someone on a minor infraction. Like, I believe one member of our first panel said a woman in Massachusetts, her landlord tried to evict her because she had her ex-husband coming in for child care. We see all sorts of fine red lines written into these contracts, and it's really a way for landlords to manipulate reality around their own interests. And I would say the same is true for public accommodations. I want to question a little bit the, you know, we see these systems, we know that retail theft is talked about a lot, and this seems to be a huge problem for pharmacies in particular. But what about the fact that Rite Aid's CEO made 20 million dollars in 2024? Where are we really seeing these costs? And if someone isn't able to pay for formula for their baby, and then is caught shoplifting, what's really the cost there compared to the millions of dollars CEOs and executives are getting paid at these companies?

CHAIRPERSON DE LA ROSA: Thank you for your thoughts on that.

I want to ask one last question on my behalf. I don't know if Council Member Hanif has some more questions. Okay.

There's a concept that we've been talking about, and it's the right to be forgotten, similar to the principle recognized in the EU, allowing individuals to request deletion of biometric data. It's technically possible with facial recognition and AI. Do you have any thoughts about that concept, and if that's something that we should be looking into?

SERGIO DE LA PEÑA: Right. It's presented as this all or nothing choice that we have to make, right? So, what are you going to do if you want that really good, well-customized running shoe, don't you want them to analyze your gait? Sure. Analyze my gait, give me the shoe, and then delete it. It's not either or. It's not permanent storage. It's not a digital footprint that lasts my lifetime. It's a transaction that I'm engaging in. If this is a useful tool, let's use it, and then at the end of it, destroy it. So, I think that's the nuance that I think is being ignored too often between like saying, well, and we see it, it's intellectually dishonest. This constant choice, we see it in the world of public defense all the time. It's like, well, don't you want safety? Don't you want public safety? Do away with this. And it's just this constant erosion of civil rights in the name of safety that it just becomes too vague, and I think it's illegitimate at its core.

SHRUTHI VELIDI: I think what I wanted to flag there is that there's not enough, I think, language talked about in terms of retention policies, and of course, the time it takes if someone requests that their data do be deleted. We're seeing a really, really large range of dates and time periods provided, ranging from two years to 45 days to 14 days. And so even if someone does request that data to be deleted, the request gets flagged into a large system, and by the time maybe their data does get deleted, maybe they forgot about it. So, sort of also making that process actually user-friendly. And we'd also like to flag that I think, similar to what my panelists said earlier, biometric data can also be used beyond the purpose of identification, right? And I think that's also something that really needs to be clear is that biometric data can be used for data analysis, behavior, sentiment recognition, right? But those theoretically can be used to flag security threats or use body, head, eye movements to monitor employees' productivity during remote work, and these are full of biases, right? And so I think part of this is also just making sure that when we do set limitations on biometric tracking technologies, we include going beyond just identification and verification, but really the whole host of biometric applications.

CYNTHIA CONTI-COOK: I'll just add that New Yorkers have a really long history of being concerned about their privacy, probably because we live on top of each other. And since 1989, there's been executive orders that have been really trying to be deliberate and intentional about what we share publicly and what we share with city agencies and what they can share about us as well. And so, 100 percent, I think now more than ever, is a time for us to really ask some hard questions, not only about the right to be forgotten in the sense that we get to write our own stories and be our own autobiographers, but also because there is a proliferation of AI technology that is scooping up information about us. So, it's no longer about am I a target of an inquiry or an investigation? It is now a question of, is what I am generating content about, whether that is content about the geographic patterns on my face or whether that is content I'm co-creating online? No matter what we are generating, it is fodder for artificial intelligence systems. And when I referenced earlier the agentic AI systems that are being rolled out, they also want to have access to biometric information. And the industry associations, of course, say that that is for the purpose of making everyone's identity safer. And at the same time, there's nothing happening in terms of regulating the amount of AI chatbots that are proliferating and creating the very chaos that they claim biometric identification will save us from. So, let's focus our efforts on regulating and preventing the chaos, and then we don't need to make decisions based in fear.

SHRUTHI VELIDI: Can I add one clarifying comment? I think just in terms of also the deletion aspect, I think one thing that's also forgotten is just because your data is deleted, but if an LLM, for example, was trained on that data, you can't delete the weights. And so there's really not really a concept of very clean, just deletion, because once these models are trained, it's very, very hard to sort of go back and use different models and change how the models are actually developed. So, I just wanted to flag that.

CHAIRPERSON DE LA ROSA: Thank you all for coming and for providing a testimony and your thoughts on this.

Up next, okay, the last panel. Beverly Blondmonville and Michele Blondmonville.

MICHELE BLONDMONVILLE: Thank you. Good morning.

CHAIRPERSON DE LA ROSA: Sorry. One second. If we could take conversations outside, that would be great. And yes, thank you. And sorry, you may begin.

MICHILE ANNE BLONDMONVILLE: My name is Michele Anne Blondmonville. I'm a health and fitness educator for 40 years, former adjunct lecturer at New York University, trainer at American Red Cross and other health facilities across New York.

I am in favor of Intro. 428 being passed and Intro. 213. As was said by the other testimonies, that once data is falsely collected, it's met with catastrophic consequences and that there's no going back with that distribution. The retrieval of biometric data is used by various agencies for also experimentational purposes. I'm speaking on behalf of everyday citizens who are Havana syndrome or anonymous health incident victims, some knowingly and others unknowingly. With the glaring awareness of the benefits afforded our diplomat counterparts helping American victims affected by neurological attacks, the Havana Act of 2021, we certainly hold fast to the notion that one day we will be free from torture, pain, invisibility, and the weaponization of technology. Everyday people, Havana syndrome victims, as compromised, have diagnosed Havana syndrome public citizens who have been unlawfully experimented on and who endure targeting in various nefarious manners.

These heinous crimes include but are not limited to organized stalking, smear campaigns, noise harassment, electronic assault from directed energy weapons, and nonconsensual human experimentation. We may not be able to stop smart cities, but we do not have to be hurt in the process. They are put on a legal list unknowingly that are distributed to various agencies for this experimentation for vindictive reasons, technological research, and political harassment. No one should have their brain interfaced or be put on an AI program for experimentation purposes. We are assaulted 24 hours a day randomly for compliance and are remote neuromonitored. We would like New York to adopt laws that protect our neural data like California laws SB 1223 and the Colorado House Bill 241058 and also repeal the CARES Act. Thank you.

CHAIRPERSON DE LA ROSA: Thank you so much for your testimony.

We have one Zoom participant.

We will now turn to our witness joining us via Zoom, the person on the Zoom, Christopher Leon Johnson.

SERGEANT-AT-ARMS: Starting time.

CHRISTOPHER LEON JOHNSON: Hello. My name is Christopher Leon Johnson. I support both bills, but I want to make this clear that I believe the City Council, I think you, Mrs. Carmen De La Rosa, I think I saw Shahana Hanif next to you, needs to start talking with the Mayor's Office to introduce two bills that will protect the app-based workers, especially after in the summertime when the unpaid deactivation bills become law, because what's going to happen, I'm surprised I saw a member of the New York Tech and Workers Alliance that was sitting in the front, the Arab American guy, he was there. He didn't speak. I'm surprised he didn't speak on this, where in the summertime, once this bill becomes local law, helped by Justin Brannan and Mr. Shekar Krishnan, that the apps will start retaliating more and start weaponizing the AI feature and facial recognition feature to start justifying deactivating not only the for-hire vehicle drivers, they're going to deactivate deliverisatas. I believe that the City Council needs to sit with both the Workers' Justice Project and the New York Tech and Workers' Alliance to help introduce some bills that will make sure that will ban the apps Uber, DoorDash, Lyft, and Grubhub, like Wonder, Relay, and all these applications that's popping up all over the city, like Empower, from using AI and using facial recognition to identify the app-based workers, because what's going to happen is that they're going to use this technology every hour or every day to start saying, well, if your face don't match, we're going to just deactivate you. And then you got to prove that you're the person that's on the app. And that's my thing. I think that the City Council need to have a sit down with both Bhairavi Desai of the Tech and Workers' Alliance and Ligia Guallpa of the Workers' Justice Project to introduce bills that will prevent this from going forward. Let's make this clear that I'm supporting, I support these bills. It's a lot of this going on where they racially profile migrants and they racially profile the minorities at these stores, especially Wegmans. But I'm surprised to see that this is all about, when it comes to facial recognition, especially the MTA, it's all about collecting data, and data means money. The corporate can say, oh, we can't sell data. They sell data under the table. Everybody knows that. That's the truth. But I'll make this clear that all the advocates made everything a pointer. I don't want to be a carbon copy. But I want to make my statement that I believe that the apps need to be regulated. And the apps like Uber, DoorDash, Grubhub, and Wonder, they need to be stopped from using AI recognition, facial recognition, and ID verification when it comes to their apps. Because this hurts not only the deliveristas and the taxi drivers, like the people that do the Uber, Lyft, and Empower. This hurts the customers. Because there's customers that go to the same stuff. I know I have a few seconds. But if you're a customer and you use Uber, even before you get on the app, they make you use your ID. They (TIMER CHIME) actually ID and ask for your face.

SERGEANT-AT-ARMS: Your time has expired.

CHRISTOPHER LEON JOHNSON: Thank you so much. Enjoy your day. Thank you.

CHAIRPERSON DE LA ROSA: Thank you so much.

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

Okay. No one is on.

Thank you, everyone, for your testimony and your time. This is a very important hearing, and we look forward to following up. Thanks, Council Member Hanif, for being my partner here today.

And this hearing is adjourned. Thank you all. [GAVEL]

CERTIFICATE

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.

CORPORATE
SEAL
NEW YORK

Date ____March 17, 2026_______________