CITY COUNCIL
CITY OF NEW YORK

---------- X

TRANSCRIPT OF THE MINUTES

Of the

COMMITTEE ON TECHNOLOGY

Jointly with

COMMITTEE ON CIVIL &
HUMAN RIGHTS

---------- X

December 8, 2025
Start: 1:12 p.m.
Recess: 4:24 p.m.

HELD AT: 250 Broadway-8th Fl. Hearing Rm. 3

B E F O R E: Jennifer Gutiérrez
Chairperson

Nantasha M. Williams
Chairperson

COUNCIL MEMBERS:
Erik D. Botcher
Robert F. Holden
Vickie Paladino
Julie Won
Rita C. Joseph
Christopher Marte
Rafael Salamanca, Jr.
Kevin C. Riley

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

Michael Fitzpatrick
Chief Privacy Officer for the City of New York,
Head of the Office of Information Privacy

Talia Kamran
Brooklyn Defenders

Clayton Banks
Silicone Harlem

Alissa Johnson
STOP

Susan Peters
Wired Tech

Alex Spyropoulos
Tech NYC

Richie Lipkowitz

Beverly Blondmonville

Michele Blondmonville

Cynthia Conti-Cook
Surveillance Resiliency Lab

Odette Wilkens
Wired Broadband Inc

Christopher Leon Johnson

SERGEANT AT ARMS: Good afternoon and welcome to today's New York City Council hearing for the Committee on Civil and Human Rights joint with the Committee on Technology. If you would like to testify, you must fill out a witness slip with one of the Sergeant at Arms. You may also submit testimony at testimony@council.nyc.gov. At this time, please silence all electronic devices, and no one may approach the dais at any time. Chairs, we are ready to begin.

CHAIRPERSON GUTIÉRREZ: [gavel] Thank you. Good afternoon. I'm Council Member Jennifer Gutiérrez, Chair of the Committee on Technology. I want to thank my colleague, Council Member Dr. Nantasha Williams, Chair of the Committee on Civil and Human Rights for partnering in today's oversight-- for agreeing to partner in today's oversight. I also want to thank the administration and our agency representative who's here to testify today. Today's hearing asks a simple but essential question. As New York City increasingly relies on digital systems, are we prepared to protect the personal information entrusted to us? Across government we are seeing extraordinary growth in the amount of data being

collected and used from MyCity and benefits enrollment systems to enforcement databases to digital services. These tools have tremendous potential. They can make government faster, more coordinated and more responsive, but as these systems expand, so must our safeguards. The city does have a privacy framework. What we are examining today is whether those pieces are working together as a coherent system, one that provides not only guidance, but also accountability, consistency, and clarity. Right now, we hear of major gaps. We cannot have a structure that depends heavily on voluntary compliance rather than enforceable standards, or one that has definitions and practices that vary widely from agency to agency. Privacy is not simply an administrative concern. It is a matter of trust and for many communities, immigrants, survivors, young people, tenants, workers, it is a matter of personal safety. It is a matter of civil rights. We also know that data sharing has enormous value when done safely. It can speed up benefits. It can reduce paperwork burdens, coordinate outreach and help ensure that vulnerable people receive timely support, but increased data sharing also increases risks. A

single breach, even one caused by a subcontractor several layers removed can expose deeply personal information. These are not abstract concerns. They have happened and have real world consequences that we must be prepared for. So, today's hearing is not about assigning blame. It is about understanding the protections we have, how they are being implemented and what additional tools or structures may be needed to keep pace. Our goal is straightforward, to ensure New York City has a privacy system that is strong, that is coordinated and capable of earning the trust of the people we serve. We will be hearing the following bills: Intro 1335 sponsored by myself, a Local Law to amend the Administrative Code of the City of New York in relation to the definitions of identifying information and private information; Intro 1340 sponsored by Council Member Louis, a Local Law to amend the Administrative Code of the City of New York in relation to an interagency taskforce and reporting on a gendered impact assessment of artificial intelligence; and Intro 1367 sponsored by Council Member Salaam, a Local Law to amend the Administrative Code of the City in relation to a top level domain name requirement or websites maintained

by city agencies; Reso 783 sponsored by my colleague, Council Member Dr. Nantasha Wiliams, resolution calling on the New York State Leg to pass and the Governor to sign Senate Bill 4860 in relation to enacting the New York Data Protection Act; and Reso 1062, sponsored by Council Member Hanks, a resolution calling on the New York State Legislature to pass and the Governor to sign, Bill 3924, also known as the Right to Your Own Image Act in relation to privacy rights involving digitization. Finally, as I near the end of my tenure as Chair of the Technology Committee, I want to sincerely thank my colleague, my partners, the agencies, advocates, and New Yorkers who have engaged with us over the past two sessions. It's been an honor to learn alongside you and to work together towards a more accessible, equitable, and responsible digital city. I want to thank, of course, our tech committee staff, Policy Analyst Erik Brown [sp?] who's here, our Legislative Irene Byhovsky, and my Chief of Staff, Anya Lehr [sp?], for their dedication to building a strong thoughtful framework for our city. And now I'm going to turn it to Council Member Dr. Williams for her opening testimony [inaudible] many things, excuse me.

CHAIRPERSON WILLIAMS: Thank you. Good afternoon, everyone. I am Nantasha Wiliams and I serve as Chair to the Committee on Civil and Human Rights. I would like to first start off by thanking everyone for joining us for today's hearing, especially my Co-Chair, Council Member Jennifer Gutiérrez. While the risk of harm inherent to the collection, storage and use of personal data must be evaluated and addressed on a society-wide level, the potential negative impacts are marginalized [inaudible] merit, particular attention, and not only because such harms are often differentiated in their scope or scale. Some organizations that study data privacy have asserted that digital privacy legislation is civil rights legislation, meaning that digital privacy protections are essential to preventing the replication and exacerbation of existing structural inequities in our digital systems and processes. The Brookings Institute, a U.S.-based global policy think tank called the right to privacy a matter of survival for marginalized groups because privacy violations have so often led to increased risk of ostracization, discrimination, or physical danger. Take for example, GoGuardian, an educational

software used for communicating of students and monitoring their online activity. It is used in many of our nation's schools including right here in New York City, and its usage has grown considerably since the COVID-19 pandemic introduced remote learning on a wide scale. While incredibly helpful to educators and students alike, some of the tracking capabilities of GoGuardian also have been cause for concern. For example, the ability to track all search history, location data, and time of usage for students flagged as "at-risk" allows for building of hyper-specific and potentially unfair biased profiles containing data that can be shared without full knowledge of the student. Similar software programs and such features have been linked to the outing of sexual orientations and/or identities due to the flagging of certain key words and search terms such as lesbian or gay, something which could potentially have dangerous or life-threatening consequences for LGBTQ+ identifying students. Additionally, city government agencies collect and store extensive individualized information necessary for service delivery, analysis, or other administrative functions of government. While all city residents face risks if their private

data is stolen or published, government-held data is likely to be more comprehensive and potentially more sensitive for individuals in communities who rely on multiple government services. Because government services are often designed to provide a social safety net, marginalized or vulnerable populations maybe more likely to access certain types of services and therefore more likely to have detailed personal data stored across city agencies. We cannot avoid technological advancement, but we can keep the door open for discussion surrounding not only its ethics, but its impacts on these vulnerable populations. I will now pass it back to my Co-chair.

CHAIRPERSON GUTIÉRREZ: Thank you so much. Today, we will hear testimonies-- oh, no. I want to quickly acknowledge our Council Members who are joining us, Council Member Bob Holden who's on the Technology Committee, Council Members Marte and Riley on the Civil Rights Committee. Today, we will hear testimonies from the New York City Office of Technology and Innovation, the Chief Privacy Officer, and I want to welcome Michael Fitzpatrick, excuse me, my apologies, Chief Privacy Officer.

COMMITTEE COUNSEL: Thank you, Chair. Good afternoon, everyone. And before we begin with the administration testimony, I just kindly ask you to raise your right hand. Thank you so much. Do you affirm to tell the truth and respond honestly to Council Member's questions?

CHIEF PRIVACY OFFICER FITZPATRICK: I do.

COMMITTEE COUNSEL: Thank you so much. You might start your testimony.

CHIEF PRIVACY OFFICER FITZPATRICK: Good afternoon, Chairs Gutiérrez and Williams and members of the City Council Committees on Technology and Civil and Human Rights. My name is Michael Fitzpatrick and I am the Chief Privacy Officer for the City of New York and the Head of the Office of Information Privacy. Thank you for providing this opportunity to address the Council about my office's critical responsibilities and significant achievements concerning citywide privacy governance. I am grateful to the Chairs for their leadership in facilitating this important conversation dedicated specifically to privacy. The role of the Chief Privacy Officer was established by Local Laws 245 and 247 of 2017, otherwise known as the Identifying

Information Law. Subsequent legislation formally established the Office of Information Privacy within the City Charter, and Executive Order 3 of 2022 placed the Office of Information Privacy within the Office of Technology and Innovation as part of the wider consolidation of technology-related offices. As Chief Privacy Officer, my responsibilities include establishing citywide policies and protocols related to agencies' collection, disclosure, and retention of identifying information, accomplished through the publication of the Citywide Privacy Protection Policies and Protocols at least every two years. My office also publishes a companion Agency Privacy Officer Toolkit to assist Agency Privacy Officers with guidance in putting policy into practice. This is comprised of written guidance on information privacy best practices, including templates and hands-on tools to standardize and scale privacy governance. Our office has published all of these materials on our website, making them available to both the public and other privacy professionals, and welcomes feedback through a dedicated form established on our website. A core objective of our office is promoting public trust in

government services, particularly through clear governance for how the city handles identifying information, supporting the confidence of New Yorkers that it is safe to seek assistance. Promoting public trust is carried out through our crucial partnership with Agency Privacy Officers who work across the city within each agency covered by the Identifying Information Law. Agency Privacy Officers are designated by their respective agency heads to be stewards of their agency's privacy practices and make decisions about how their agency collects, discloses, and retains identifying information. My team supports Agency Privacy Officers in their day-to-day work as they navigate compliance with privacy laws and policies. Our office regularly advises on appropriate privacy provisions for data-sharing initiatives and contracting terms for use with vendors, and provides privacy trainings on updates to law, policy, and best practices. Each Agency Privacy Officer also prepares and submits biennial reports to my office, as well as to the mayor and speaker of the council, concerning their policies and practices related to identifying information. These reports are reviewed by my office and provided to the Citywide

Privacy Protection Committee to support their development of recommendations for improving the city's privacy policies. In 2023, the Citywide Privacy Protection Committee's charge expanded beyond solely the review of biennial agency privacy reports to an ongoing advisory role on matters relating to emerging technology and current events to further enhance citywide privacy practices. In support of that objective, agency heads for city agencies with committee membership were asked to assess their designees who serve on the committee, and committee membership was diversified beyond agency privacy professionals to include information technology, information security, technology policy, and data analysis professionals. Additionally, two-year terms for agency designees were established, aligning ongoing assessment of committee needs with the biennial review schedule. Based on Citywide Privacy Protection Committee recommendations, the Citywide Privacy Protection Policies and Protocols and Agency Privacy Officer Toolkit were updated in 2023 and 2025. These updates included: minimum standards for individual notification and identity protection services; enhanced privacy-related contract terms;

privacy by design guidance, a collaborative process that embeds privacy protections directly into the foundational architecture of technologies, systems, and business processes at the earliest stages of the project lifecycle; reporting unauthorized disclosures of identifying information within 24 hours of Agency Privacy Officer discovery; several new governance models and template documents; and minimum standards for receiving complaints under the Identifying I Law. I am also proud of recent professional development initiatives of my office which have significantly advanced the citywide information privacy program, examples of which include: One hundred percent of our full-time staff obtaining at least one certification by the International Association of Privacy Professionals, and providing IAPP membership credentials to every Agency Privacy Officer, which provides access to materials in support of their professional development; expansion and diversification of staff through the hiring of program management and privacy analysis positions, in addition to three full-time CUNY Technology Empowering Careers Fellows to implement tools in support of data-informed program enhancements;

convening the first Agency Privacy Officer Summit, inviting all Agency Privacy Officers and their staff for a full-day program of discussions and panels demonstrating privacy policy in practice; and establishing a "Privacy in Practice" externship program in partnership with Fordham Law School, training emerging privacy lawyers in public service privacy frameworks while developing members of our office as adjunct professors of law. Additionally, we've elevated awareness of the citywide information privacy program both within New York City and beyond in a variety of ways, through news coverage and promotion on multiple, public-facing communications channels including social media, through our observer status in the Global Privacy Assembly, and through our service as New York City's representative to the Cities Coalition for Digital Rights. These achievements would not have been possible without the exceptional work of our staff at the Office of Information Privacy, the strength of our Agency Privacy Officer community, and the diligence of the Citywide Privacy Protection Committee, and collaboration with our colleagues at the Office of Technology and Innovation. I am grateful for their

partnership in strengthening information privacy governance in New York City. Now I will turn to the legislation being considered on today's docket. Introduction 1335 of 2025 would amend the Identifying Information Law definition of identifying information, and the local, security breach notification law's definition of private information. As the Council is aware, the city defines identifying information as any information obtained by or on behalf of the city that may be used on its own or with information to identify or locate an individual. The law contains an illustrative list of the types of information defined as such identifying information, and it affords the Chief Privacy Officer with the authority to designate additional types of covered information. Updates to the Citywide Privacy Protection Policies and Protocols reflect such designations and include categories covered by the language this bill proposes to add to the Identifying Information Law, specifically gait and movement patterns, like keystroke, and device identifiers. Therefore, I do not have objections to these particular additions to the list of types of identifying information. However, we are assessing

the potential operational impact of the proposed language that would designate certain technological information as private in the context of breach notifications in Ad Code 10-501. I'm happy to discuss this further with the Council. Introduction 1340 of 2025 would require OTI to conduct a gendered impact assessment of algorithmic tools every two years and participate in an interagency task force on the gender equity of artificial intelligence tools in the workforce. Less than two weeks ago, the Council passed a comprehensive package of legislation in part aimed at identifying bias in algorithmic and artificial intelligence tools, which I understand the Council and the administration negotiated in good faith. If further discussion is needed in the AI and algorithm space, I urge the Council to engage with my colleagues in the Research and Collaboration team at OTI. Finally, Introduction 1367 of 2025 would require agencies to adopt .gov domain names for public-facing websites. OTI agrees with this proposal in concept in that it is good practice to have a trusted and uniform URL for government websites. This legislation is already under review by my colleagues in Infrastructure Management,

Applications, and Strategic Initiatives, all of whom play a part in the city's public-facing websites, and I would defer any further discussion of this legislation to them. I am now happy to take Council Members' questions regarding the Identifying Information Law and the city's privacy governance.

CHAIRPERSON GUTIÉRREZ: Thank you. Thank you so much for that detailed testimony. I do have some follow-ups about the bills that we're hearing today. But just to start, I just want to start with some basic context so we can have it on the record. Can you please state your name, your title, and any legal or professional qualifications to serve as the citywide Chief Privacy Officer?

CHIEF PRIVACY OFFICER FITZPATRICK: Absolutely. My name's Michael Fitzpatrick. I'm New York City's Chief Privacy Officer. I have-- I'm a graduate of Fordham Law School holding a Juris Doctor. I hold a Master's in Cyber Security Risk and Strategy from NYU. I hold privacy certifications from the International Association of Privacy Professionals and U.S. Law and Privacy Program Management, as well as been designated as a fellow of Information Privacy by the IAPP. I have served as a

tenure on the U.S. Department of Homeland Security Data Privacy and Integrity Advisory Committee.

CHAIRPERSON GUTIÉRREZ: Great.

CHIEF PRIVACY OFFICER FITZPATRICK: Those are immediately what come to mind.

CHAIRPERSON GUTIÉRREZ: No, no, excellent. I just wanted to stress your technical qualifications for the, like-- the breadth of this position and how vital it is to have someone who knows what they're talking about.

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you for that opportunity.

CHAIRPERSON GUTIÉRREZ: Thank you. Yeah, yeah, of course. Can you share what is-- how large is your particular office? How many personnel? How many people work there, and the core function?

CHIEF PRIVACY OFFICER FITZPATRICK: Absolutely. We have a current active staff of nine full-time employees.

CHAIRPERSON GUTIÉRREZ: I think-- including you.

CHIEF PRIVACY OFFICER FITZPATRICK: Including me.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: In addition to those nine, we have the three CUNY Tech fellows that I mentioned in my testimony, and we currently have three vacancies which we're actively looking to fill.

CHAIRPERSON GUTIÉRREZ: Can you share what are those positions for the vacancies?

CHIEF PRIVACY OFFICER FITZPATRICK: We have a Special Counsel for Information Privacy position, and Associate Counsel position, and a Privacy Analyst position.

CHAIRPERSON GUTIÉRREZ: Oh, okay. And the CUNY fellows, how long are they there for?

CHIEF PRIVACY OFFICER FITZPATRICK: We have them for three years.

CHAIRPERSON GUTIÉRREZ: Oh, excellent.

CHIEF PRIVACY OFFICER FITZPATRICK: They're-- we're just over the first year with them.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: And they have done such fantastic work. You know, being folks who come into this without necessarily having any information privacy experience, but bringing unique experience nonetheless, and the attitude of

learning like we all do as privacy professionals every single day.

CHAIRPERSON GUTIÉRREZ: Excellent. That's great. That's encouraging to hear. Can you share how many agencies you consult with on privacy matters or how many agencies have privacy officers that exist across city agencies?

CHIEF PRIVACY OFFICER FITZPATRICK: Of course, Council Member, Chair. We have-- from a biennial reporting perspective, we received 126 agency reports in 2024. Within the bounds of that include entities that submit one report, but are comprised of multiple offices, principally the Mayor's Office. We receive one report from the Mayor's Office, but there are privacy liaisons distributed across the component parts with one privacy officer existing at City Hall. Through that lens, we maintain a privacy network in excess of 175 across the broader New York City ecosystem, and that includes with Community Boards.

CHAIRPERSON GUTIÉRREZ: Okay. And so, of the-- that's 175 agencies and/or office, like Mayor's offices, and of those 175--

CHIEF PRIVACY OFFICER FITZPATRICK: [interposing] That's correct.

CHAIRPERSON GUTIÉRREZ: Oh, okay. It's right. You nodded. And of those, do every single one of them have a agency Privacy Officer?

CHIEF PRIVACY OFFICER FITZPATRICK: The 126 number would be the universe of Privacy Officer.

CHAIRPERSON GUTIÉRREZ: Okay, okay. Is there-- can you explain if there's a reason for why it's 126 out of the 175 that have agency Privacy Officers, besides like the Mayor's Office. I get that.

CHIEF PRIVACY OFFICER FITZPATRICK: Well, it is principally the Mayor's Office that results in that delta, because there are so many separate offices comprised of--

CHAIRPERSON GUTIÉRREZ: [interposing] Oh, so that difference of like 50 or so are just the various mayoral office.

CHIEF PRIVACY OFFICER FITZPATRICK: I believe that's correct.

CHAIRPERSON GUTIÉRREZ: Okay, so every other agency has and APO.

CHIEF PRIVACY OFFICER FITZPATRICK: That's correct.

CHAIRPERSON GUTIÉRREZ: And I know you said this in your testimony, but can you just-- if there's any more information you can share who appoints the agency privacy officers?

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you for that question, Chair. Those designations are made by the agency head.

CHAIRPERSON GUTIÉRREZ: So, the Commissioner?

CHIEF PRIVACY OFFICER FITZPATRICK: That's correct.

CHAIRPERSON GUTIÉRREZ: Okay. Do you-- are those designations, are they made in-- is there anyone that they're consulting with? Are they consulting with you, with anyone at OTI, about those designations?

CHIEF PRIVACY OFFICER FITZPATRICK: On a voluntary basis, we updated the policies in 2025 to strongly encourage agency heads to consult with the Chief Privacy Officer given the critical role these folks play at their agencies, but it is a voluntary encouraged element of city policy.

CHAIRPERSON GUTIÉRREZ: Okay. What qualifications are required? Or I guess when they consult with you voluntarily, let's start there, because I realize it's not every agency. If and when they consult with you, what are some of the qualifications that you are looking at.

CHIEF PRIVACY OFFICER FITZPATRICK: So, that's a really question, Chair. You know, not-- I recognize not everybody is going to have the same kind of background and credentials that you provided me with the opportunity of sharing--

CHAIRPERSON GUTIÉRREZ: [interposing] That are extensive.

CHIEF PRIVACY OFFICER FITZPATRICK: earlier. But I look for, you know, elements of privacy practice. You know, there are folks that, you know, very often are engaging in work at their agency level that has privacy equities, that they may not necessarily even think about them. So, I look for those sorts of skills. I look for certainly interest in the subject matter.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: You know, often that's a conversation about the state of

the profession, you know, issues of the day. Where do we see, you know, privacy practice going in the next five years. And from there, you know, I'm able to, you know, assess and provide feedback to agencies when I'm consulted on those types of--

CHAIRPERSON GUTIÉRREZ: [interposing] Are there-- thank you for that. And just so that I'm clear, the agency privacy officers, is the work of-- the bulk of their work is this designation full-time ore are they also expected to do anything else?

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you for that question, Chair. The identifying information law provides that APOs can do other things. We actually recently did a survey of the APO community, voluntary survey, of course, but we've received information back that I think is quite important. You know, our APOs are generally spending-- of those who responded to the survey, less than 50 percent of their day on privacy policy--

CHAIRPERSON GUTIÉRREZ: [interposing] [inaudible]

CHIEF PRIVACY OFFICER FITZPATRICK: work, and they've also shared that additional staffing investment in those types of work streams would be a

benefit to them. And for us as an office of information privacy, you know, recognizing, you know, where even at the nine current full-time employees, we're dedicated to this work full-time, and what we endeavor to do is try to scale as much as we can to support APOs recognizing that that is the operational environment that is their day-to-day.

CHAIRPERSON GUTIÉRREZ: Okay, that's great. And the survey that you shared, when was that-- - that was done this year in 2025?

CHIEF PRIVACY OFFICER FITZPATRICK: Yeah.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: That survey I believe was in October.

CHAIRPERSON GUTIÉRREZ: Oh, okay, just recently. What are-- what were some of the other questions if you remember that you all asked?

CHIEF PRIVACY OFFICER FITZPATRICK: I'm happy to provide the survey, but it was-- this particular survey was coming out through this perspective of resources for APOs.

CHAIRPERSON GUTIÉRREZ: Needing more resources, okay.

CHIEF PRIVACY OFFICER FITZPATRICK: Or distilling that universe of information out so that way, you know, we as an Office of Information Privacy and continue to advocate like, for example, obtaining those IAPP memberships for every APO, which we distribute as part of the onboarding exercise whenever a new APO is designated.

CHAIRPERSON GUTIÉRREZ: Yeah, okay. Thank you. And then you've been the Chief Privacy Officer I guess the entire duration of this administration, correct, almost?

CHIEF PRIVACY OFFICER FITZPATRICK: Almost. My--

CHAIRPERSON GUTIÉRREZ: [interposing] Shy of a few months.

CHIEF PRIVACY OFFICER FITZPATRICK: My predecessor retired I want to say February of 22.

CHAIRPERSON GUTIÉRREZ: Okay, yeah.

CHIEF PRIVACY OFFICER FITZPATRICK: And I came into the role April of 22.

CHAIRPERSON GUTIÉRREZ: Okay, and in that time would you be able to share how many times agencies have voluntarily reached out about wanting

assistance or just to review as they were appointing Agency Privacy Officers?

CHIEF PRIVACY OFFICER FITZPATRICK: I can come back with a more definite answer on that, but--

CHAIRPERSON GUTIÉRREZ: [interposing] What would be the reason, if I'm a Commissioner? Maybe I don't have this. I don't have a fraction of the background that you have. What would be the reason that I wouldn't go to the City's Chief Privacy Officer to appoint an Agency Privacy Officer? Like, what-- I'm just trying to under-- I get that it's voluntary. I disagree that it should be voluntary, but I'm trying to see, trying to understand if I'm not an expert in this, why I wouldn't go to the expert for this.

CHIEF PRIVACY OFFICER FITZPATRICK: So, a great question, Chair. You know, I think agencies and their Commissioners, you know, certainly have, you know, authority to make personnel decisions within their ecosystem. You know, for us, and it's part of the broader work that we endeavor to do citywide. We want to cultivate that space where folks do feel comfortable coming to us, and I think being a value add to the conversation, that

particular element that I mentioned earlier about strongly encouraging that engagement. You know, we are just approaching about a year where that has been the case, and obviously we've got, you know, a number of instances where that either has or certainly has not happened, and certainly I'm prepared to have that inform further policy steps and enhancement.

CHAIRPERSON GUTIÉRREZ: I'd love to see what that ratio is, and also just considering the amount of breeches that various of our agencies have had, wanting to really trust someone like yourself with your background on those recommendations. Do you-- in your opinion, do you think it's something that should be mandatory, that there should be a consultation, a formal kind of joint assessment before making that designation with someone of your position?

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you for the opportunity to speak on that.

CHAIRPERSON GUTIÉRREZ: You can be honest. You only got a few weeks under this administration--

CHIEF PRIVACY OFFICER FITZPATRICK: [interposing] No, I--

CHAIRPERSON GUTIÉRREZ: without little retribution.

CHIEF PRIVACY OFFICER FITZPATRICK: I appreciate the opportunity. You know, I think, you know, the-- we certainly endeavor to be a value-add in all of those decisions, and we've been fortunate not just through the investments that have been made along this administration, you know, some of which I've outlined earlier, but afforded the opportunity to socialize among the Commissioner universe, the importance of the Agency Privacy Officer. You know, it's going back in the earlier days of the admin--

CHAIRPERSON GUTIÉRREZ: [interposing] But yes or no, do you think it should be mandatory?

CHIEF PRIVACY OFFICER FITZPATRICK: I--

CHAIRPERSON GUTIÉRREZ: [interposing] That there should be consultation. There should be some kind of like a process as the Chief-- the City's Chief Privacy Officer when agencies-- as you said, every single agency, 126 of them, have an APO, that you're vetting them, that you or your team are vetting them?

CHIEF PRIVACY OFFICER FITZPATRICK: I don't know that I would characterize as vetting. I

would certainly, you know-- I welcome the opportunity to be involved in as many of these types of conversations as we can be. And certainly, you know, any ongoing assessment of performance related to privacy officers, we have a front row seat to that, and obviously can have a perspective that I think would be a helpful one.

CHAIRPERSON GUTIÉRREZ: Of course, okay. I have a couple more questions, and then I'm going to-- I have a lot more questions, but I'm going to ask two more and then I'm going to pass it on to my colleague. Okay, so sorry. Okay. Under the city's current privacy framework, can you share with me the role that you and your team have in compliance when it comes to a harmful data practice by an agency?

CHIEF PRIVACY OFFICER FITZPATRICK: Can you expand on harmful--

CHAIRPERSON GUTIÉRREZ: [interposing] sure, sure, sure. I guess if an agency has found that they're-- and I know that they're self-reporting this, but when there is some violation of a privacy standard, and I know you have this awesome extensive toolkit. So, flowers to you and your team for putting that together. But when there is evidence

that there's been some violation, what role does your office play when that is disclosed to you? Kind of what is that-- what does that process look like? Let's start there.

CHIEF PRIVACY OFFICER FITZPATRICK: Absolutely. Absolutely. So, you know, we at our core and wear an advisory services hat, but that also, you know, includes facilitating of information sharing related to privacy governance within the broader ecosystem. You know, that manifests, for example, the quarterly reports when things have not gone according to plan. That information is prepared by the Chief Privacy Officer and submitted to the Council. The biennial agency reports, obviously those reports go to not just me, but to the Mayor and to the Speaker of the Council, you know, providing visibility into what those agency practices are. Similarly, the recommendations that are developed by the Citywide Privacy Protection Committee, after review of those reports are equally shared with the Mayor, Speaker of the Council, and myself. So, you know, that's the broader universe of how, you know, we distribute information across the ecosystem and in terms of accountability. With respect to the

specific work that we do when we receive an agency report, that information has been shared in an authorized manner. We're engaging directly with the Agency Privacy Officer to understand the circumstances at play. That can include engaging other partners within the Office of Technology and Innovation, particularly if there is an information security nexus. We'll work in partnership with our colleagues at the Office of Cyber Command, driving at understanding what's occurred, driving at remediation--

CHAIRPERSON GUTIÉRREZ: [interposing] Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: and to the extent that the universe of compromised involves elements that-- data elements where law requires individual notification or if prudential notification is advisable under the circumstance, we facilitate that work stream and support agency privacy officers in regard. Of note, Chair, if you'll indulge me, this is one operating practice that we've implemented over the course of my tenure as Chief Privacy Officer, and we're able to do it by virtue of the expanded headcount that we've had.

We're at nine. When I started we were five, including me. And so, getting those additional-- that additional staff inclusive of attorney members on staff has allowed for us to have counsels which maintain dedicated relationships with APOs across the city. We've got folks on staff who maintain these are your list of agency clients, you're responsible for regular engagement with them--

CHAIRPERSON GUTIÉRREZ: [interposing] Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: when those reports come in. That relationship exists, you know-- we want to have an operating structure where that is not the time where folks are getting to know one another. We're talking. We understand. We understand what we've got to do, and so that's, you know, a critical element of our work in responding to those circumstances.

CHAIRPERSON GUTIÉRREZ: How many-- so I think that's great. I think that makes sense. And so-- but how-- and how many counselors do you have now?

CHIEF PRIVACY OFFICER FITZPATRICK: Right now we have three senior counsels, one associate counsel.

CHAIRPERSON GUTIÉRREZ: and then you're looking to hire two more, three more?

CHIEF PRIVACY OFFICER FITZPATRICK: We're looking to hire two more, and then members of my executive staff are also attorneys.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: My Deputy Chief Privacy Officer and Executive Director.

CHAIRPERSON GUTIÉRREZ: Okay. Okay. Either way, just people that would be able to foster those relationships. Excellent. And how are they-- I know that you're obviously-- you don't have the full team that you'd like to right now. How are you dividing, I guess, the agencies that they're working with? Obviously, I think some agencies interface with, you know, potential data threats more than others. How are those-- how are those assigned?

CHIEF PRIVACY OFFICER FITZPATRICK: So, thank you for that question, Chair. You know, when you think about distributing that large universe over across, you know, a smaller-- we have to make

difficult decisions on what that looks like, and we tyr to do that in a way that balances, you know, historic engagement with the agencies concerned--

CHAIRPERSON GUTIÉRREZ: [interposing] Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: complexity. You know, does the agency deal with regulated data, for example. But we also critically factor the professional backgrounds of our senior counsels. When we had this initial expansion, we were looking for folks who didn't have the same exact pedigree. And so, in doing so, you know, we've brought folks on board who have extensive experience working in private sector technology.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: Folks who have experience working in prosecutor's office at both the local and state level. And then folks who, you know, had experience within the New York City ecosystem, not specifically dedicated to privacy. Each of those personnel bring a unique experience that helps inform how we make the decisions about who to assign as clients as we refer to them.

CHAIRPERSON GUTIÉRREZ: Excellent. It sounds thoughtful. And so just that I am clear on the process. I mean, you gave a really a thought-- a really detailed answer. I think it's extensive, how you and your team will step in the instance of a data violation. So, let me just-- I took a couple notes. So, it's obvious you're facilitating support. There's mediation if necessary. What is the path to getting them to be compliant or to meet those like compliance standards thereafter?

CHIEF PRIVACY OFFICER FITZPATRICK: Sorry, can you--

CHAIRPERSON GUTIÉRREZ: [interposing] Yeah, if there's a violation, your office-- you've been-- that's been disclosed. Your office is now working with them. You're mediating. What is the-- like, what are the specifics that you can share to get that particular agency back to being compliant-- to avoiding that violation in the future?

CHIEF PRIVACY OFFICER FITZPATRICK: You know, I think it's largely achieved through, you know, those good times communications that we do, you know, before a report comes in. it really does foster an environment where, you know, we want to get it

right. We've got a circumstance that we're responding to. How do we address? How do we get back to the place that we should be. We're not-- you know, and have not found ourselves in a position where, you know, we've got to give directives on remediation. That's really just not been our posture, because we haven't needed it to be.

CHAIRPERSON GUTIÉRREZ: Okay. And do you-- are you empowered to do so, to give directives in those instances?

CHIEF PRIVACY OFFICER FITZPATRICK: Yes.

CHAIRPERSON GUTIÉRREZ: And so there is a standard of compliance, and when a violation is this close to you, and your team, are you-- can you say that you're able to mandate that the fall-- like follow this path of compliance after you've worked with the? Is it mandatory for them? Is it mandatory for an agency that has disclosed a violation to follow, you know, your-- the kind of the best practices or however you design their pathway back to compliance?

CHIEF PRIVACY OFFICER FITZPATRICK: I think it would depend on the circumstances. So, for example, you know, if--

CHAIRPERSON GUTIÉRREZ: [interposing] Can you tell an agency to stop a practice if you don't think it's safe?

CHIEF PRIVACY OFFICER FITZPATRICK: It depends on the circumstance.

CHAIRPERSON GUTIÉRREZ: Okay. But you can do that? Okay. And what are-- I mean, can you give an extreme example? I know it sounds like it hasn't happened, but is there-- can you share an extreme example?

CHIEF PRIVACY OFFICER FITZPATRICK: Sure. So it's-- you know, I think that Chief Privacy Officer authority is strongest within the bounds directing implementation of anonymization techniques within, you know, a particular-- or data minimization techniques within a particular agency practice. So, you know, if there's a disclosure and that disclosure is manifested from specific elements, and that's an outcome that has not been approved by the Agency Privacy Officer directing the implementation of appropriation anonymization and minimization techniques in response to that condition.

CHAIRPERSON GUTIÉRREZ: And you're-- and you're able to do that directly or through collaboration with APO for that agency?

CHIEF PRIVACY OFFICER FITZPATRICK: I'm speaking directly to the authority reserved to the Chief Privacy Officer in that space.

CHAIRPERSON GUTIÉRREZ: Okay. Okay. Okay. Thank you for that. We just wanted to clarify how the APOs are being supported, and again, how to empower your role and your team's role in this like ever-changing time. Okay. The next one, I just want to ask about the Agency Privacy Officers. You said that there is currently an APO in every city agency-- in every city agency.

CHIEF PRIVACY OFFICER FITZPATRICK: Subject to the identifying information law. There's a list of agencies in-- I forget which specific appendix to the citywide policies that the Law Department has advised are not subject to the IIL.

CHAIRPERSON GUTIÉRREZ: Yeah. There's like 20 or so of those agencies. Okay. Can you share what is a reason why they're not--

CHIEF PRIVACY OFFICER FITZPATRICK: [interposing] That opinion is a legacy one that

predates me, so I'm, you know, unfortunately unable to share the particular rationale. As I understand it at least in part, you know, entities on that list include entities that are subject to federal privacy regulation.

CHAIRPERSON GUTIÉRREZ: Some of that are law enforcement which I understand. Some of them are I think the District Attorney's offices of every borough, I think I saw. Also saw SCA, the School Construction Authority. Just wanted to see if you were aware of any reasoning for why that is the case?

CHIEF PRIVACY OFFICER FITZPATRICK: I'm not, but getting a refresh on that particular opinion has certainly been on our to-do list.

CHAIRPERSON GUTIÉRREZ: Okay, excellent. Oh, NYCHA is also on there? Oh, wow. Okay. To your knowledge, does any agency current have a vacant APO role right now?

CHIEF PRIVACY OFFICER FITZPATRICK: Not to my knowledge. We have a protocol where when those vacancies are coming--

CHAIRPERSON GUTIÉRREZ: [interposing] Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: they're supposed to let us know as early as they can, because we want to be-- we want to have visibility where there's a gap. We want to make sure that there isn't one. You know, if we're hiring somebody new from the outside to fill the role, for example, who's going to be fulfilling those responsibilities on an interim basis, and if that is the case, conducting a full onboarding that we would for any APO, you know, proper even for an interim one, making sure they get a full one-on-one training.

CHAIRPERSON GUTIÉRREZ: It's called 101?

CHIEF PRIVACY OFFICER FITZPATRICK: APO 101.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: That's what we call it.

CHAIRPERSON GUTIÉRREZ: Is that the one that you mentioned in your testimony?

CHIEF PRIVACY OFFICER FITZPATRICK: No. Well, there-- it is among them.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: It is among them.

CHAIRPERSON GUTIÉRREZ: Okay. And then for the agencies where the APO has another title, pretty much, can you share some examples of what these other roles are in their agency?

CHIEF PRIVACY OFFICER FITZPATRICK: I think-- and it would be hard to be empirical about this, but I think the one that, you know, anecdotally we see most common is the intersection with Records Access Officer.

CHAIRPERSON GUTIÉRREZ: The intersection with?

CHIEF PRIVACY OFFICER FITZPATRICK: Records Access Officer.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: I mean, we also see, you know, legal services, attorneys within, you know, the in-house council's office at respective agency. You know, that's also a frequent.

CHAIRPERSON GUTIÉRREZ: Okay. Thank you. And so, who oversees these APOs agency to agency? Is it the agency commissioner?

CHIEF PRIVACY OFFICER FITZPATRICK: That's correct, I'm sorry. That's correct. you

know, the day-to-day supervision in management responsibility is occurring at the agency level.

CHAIRPERSON GUTIÉRREZ: And do you know who they report to? Is it the Commissioner? Is it General Counsel?

CHIEF PRIVACY OFFICER FITZPATRICK: It would depend on the agency.

CHAIRPERSON GUTIÉRREZ: Oh, okay. So, every agency has like their own hierarchy, I guess, or their own structure pertaining to the APO, okay. Would it be helpful to have something that's more uniform agency to agency? It worries me that there is just kind of like every agency is just kind of doing their own thing and treating their APO in whichever which way they want. There's like there's no consistency with respect to reporting.

CHIEF PRIVACY OFFICER FITZPATRICK: So, certainly, and thank you for the opportunity to speak on this issue, Chair. You know, I have and the work of our office has been to always try to elevate the posture of the Agency Privacy Officer as best that we can in supporting them to do their work, because we certainly view their work as important. You so, we do that and have endeavored to try to do that by

including among other things meetings with and between the Agency Privacy Officer and their agency head on our road map of checklists within the toolkit.

CHAIRPERSON GUTIÉRREZ: It's a great toolkit.

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you.

CHAIRPERSON GUTIÉRREZ: I'm just-- I mean, I'm just concerned that this is a very vital role. Obviously, a goal of our committee is to be able to expose the importance of your role, of the APOs for every agency. And I just-- I think it's not helpful if there's no consistency or uniformity. I mean, the toolkit, I think it says it on the first couple pages is voluntary for any agency or any APO to utilize, and it's very useful. There's a bunch of, you know, templates in there. There's checklist. I think it's useful. So, I'm just trying to gauge with you kind of the pathway to making this more formal, more empowered, in many ways making it more uniform and more mandatory if possible.

CHIEF PRIVACY OFFICER FITZPATRICK: Certainly. I am aligned and supportive of work that

would continue to elevate Agency Privacy Officers, you know, operations within their agency and the attendant support that's provided to them.

CHAIRPERSON GUTIÉRREZ: Okay. So, very diplomatic way of responding to that. Thank you. Okay. I have some more. I'm going to pass it to my colleague, Council Member Wiliams, for her questions.

CHAIRPERSON WILLIAMS: Thank you. I'm going to turn my questions to bias and equity in data privacy. So, can you please describe the city's policies and current approach to the use of AI an the extent to which different agencies are researching, developing or already using artificial intelligence in their day-to-day operations and when providing services?

CHIEF PRIVACY OFFICER FITZPATRICK: So, thank you for the opportunity, Chair Williams. You know, from the Office of Information Privacy's perspective, you know, the ability to collaborate and provide support within the broader AII governance ecosystem, it's one of I think the many benefits to our home being the Office of Technology and Innovation. As the AI Action Plan and attendant policy documents, you know, have been developed by

our colleagues in the Office of Research and Collaboration, we've been able to offer our perspective, and I think most significantly create that through-point within that universe of policy to our existing universe of policies, you know, citywide. Responsive to that and to a point that you raised earlier which is an important one, is in the operation of identifying whether or not, you know, data use is resulting in bias. I completely agree with you that that type of assessment is critical, certainly from an information policy perspective. It is why in 2023 we added equity to the list of New York City's privacy principles, recognizing that by virtue of the line of business that we are in, we are necessarily going to be holding identifying information of some folks more than others, and that should be a necessary element of consideration and broader decision making related to information privacy.

CHAIRPERSON WILLIAMS: Thank you. When an agency is looking into or launching a new data processing tool-- example Chat bot-- a new way to process applications, etcetera. What citywide policies or steps must it follow before launch and

what kind of testing is required and what kind of benchmarks must be met?

CHIEF PRIVACY OFFICER FITZPATRICK: So, thank you for that particular question. You know, the technical universe is distributed across, you know, a broader universe of operational folks, you know, within city service. From an information privacy perspective, you know, at the core is an evaluation of whether or not the activity being considered involves a collection or disclosure of identifying information. If the answer of that is yes, then we should operating in the space where there is Agency Privacy Officer engagement, and as we've been discussing, you know, those are the folks who are positioned and on the front lines to make those decisions at the agency level, inclusive of compliance with our citywide privacy policies.

CHAIRPERSON WILLIAMS: Thank you. And when contractors are using these types of systems, how are these systems vetted for compliance with the city's best practices?

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you for the opportunity to talk about the great work that we've been doing from a contracting lens.

Among, you know, the work streams of our office is to set forth contracting terms that help address privacy risk within the city's ecosystem. And we've strengthened those terms over the course of my time as Chief Privacy Officer and with the great work of our office, particularly in our 2025 update, reserving additional protections from an audit perspective, requiring that in our identifying information rider, rather, which must be attached to contracts under covered circumstances, that the contractor in question is committing to performing a privacy audit at least annually and additional rights from a privacy perspective if that contractor has disclosed identifying information in an unauthorized way, visibility on the New York City side of that engagement to obtain information about what the contract is doing in that space.

CHAIRPERSON WILLIAMS: And a follow-up to that, what is the oversight within the agencies over contractors? So, you know, when they're giving a set of like policies to comply with, and then what is the oversight look like for the collection, storage, and use of that data? And once they're actually

contracted, is there like a regular-- is it the APOs that are like tracking the contractor?

CHIEF PRIVACY OFFICER FITZPATRICK: It would be the Agency Privacy Officer involved in the engagement concern.

CHAIRPERSON WILLIAMS: Okay, thank you. Is it ever possible for contractors to hold onto the data after their contract with the city is finished? And to do contractors ever sell data they've collected on behalf of the city?

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you for the opportunity to speak on that issue, Chair. The prohibition on the sale of identifying information has been an element of our mandatory contracting terms for quite some time.

CHAIRPERSON WILLIAMS: And holding onto the data, no? Are they-- like, when their contract is over are they supposed to--

CHIEF PRIVACY OFFICER FITZPATRICK: [interposing] Data retention-- apologies. Data retention is also an element of our contracting terms.

CHAIRPERSON WILLIAMS: So, do they have to like confirm that they destroyed the data? Like, how do you track that?

CHIEF PRIVACY OFFICER FITZPATRICK: The agency maintains the ability to request destruction of data under the contract pursuant to the terms that we're talking about.

CHAIRPERSON WILLIAMS: Thank you. The citywide privacy protection policies and protocols, as you so eloquently stated, sets out equity as one of its privacy principles. Can you please describe how the equity principle is put into practice in your day-to-day operations and how you work with different types of city agencies to support equity and data management?

CHIEF PRIVACY OFFICER FITZPATRICK: So, that's a great question, Chair. You know,-- and I think a layered one, and it's dependent on the engagement, you know, that we might have in a given circumstance. You know, if we're talking about data sharing, you know, we're thinking about it through the ecosystem contemplated. Are we talking about, you know, New York City agency to New York City agency? If we're talking about that, you know, what

is the underlying purpose of the data sharing that's contemplated? We're asking questions about the circumstances in which that data was originally provided to the agency that's holding it, trying to distill out the context that was available to the person at the time so that we can calibrate that as an element of evaluating whether or not additional notice might be the advisable thing to do if that information sharing is going to occur. So, that's just kind of, you know, high level, but hopefully an illustrative way that we think about--

CHAIRPERSON WILLIAMS: [interposing] Yeah.

CHIEF PRIVACY OFFICER FITZPATRICK: it.

CHAIRPERSON WILLIAMS: Yeah, and this wasn't a question that was already pre-prepared, but in listening to you speak, like, using an example of something that's like a hot button topic in the Council, like the gang database. There's data that the Police Department is collecting on individuals that end up on this list. Some people argue that it's not a fair list. It's an inequitable list. And so like, is that something that your office would provide oversight on or like monitor, or you know-- because some people-- I can see an argument for

someone saying well, here's a management system that is not following the principle of equity. I mean, I don't know. But like, how could-- using that example, can you give some more like insight on how your office might assess a particular agency's usage of data that they're collecting?

CHIEF PRIVACY OFFICER FITZPATRICK: So, thank you for that broader context, Chair. You know, for-- as a matter of citywide policy, you know, that also starts to lend itself into kind of the compensating controls space. So, you know, at our threshold as we've talking about, it's that Agency Privacy Officer approval under the Identifying Information Law. The Identifying Information Law is clear about providing a lens in which those approvals can occur. It's with-- it's either required by law where the APO's determined that a disclosure is in the mission or purpose of their agency, or it's with the consent of the individual who's provided their information. You know, from a government's perspective, when we're talking about sensitive identifying information which is a term of art that we've long had, you know, that's identifying information which carries an elevated risk of harm to

an individual, and if that circumstance is manifest, additional controls are result. That includes any-- as a matter of policy, any transactions associated with that information must be subject to a data sharing agreement which-- of which we have minimum requirements for, you know, what needs to be in those agreements. And you know, those requirements don't exist by accident. They exist in furtherance of trying to distill out these very important elements associated with, you know, these types of initiatives.

CHAIRPERSON WILLIAMS: Yeah, and you've kind of alluded it-- alluded to this, too, in terms of like cross-sharing with agencies. So, I still am not sure if this is like a factual thing or not, but reports that gang database data is shared to other agencies. So there was this claim for-- around Victim Services. Victims who are on the gang database, it was brought to our attention a while ago that they get denied for victim services resources because they're on this gang database, but the Victim Services is in a different agency than the NYPD. So, even looking at that, like is that what you're saying? There's-- not is like an agreement between

agencies? Like, how does that information potentially get shared with other agencies to be used, I feel like, in discriminatory ways. Like, it's one thing to create a argument that the gang database somehow helps to address crime and preventative crime, but why does it matter if someone who may not even be affiliated with a gang, but maybe has a cousin that's a gang member and I don't know, maybe he walked down the street and somehow their name gets in the-- you know, ends up on the list, but then they're not eligible for services from a different agency. And again, I don't-- I still have not been able to figure out like if this is factual or not, but this is something that was said to me and a few Council Members by different nonprofit organizations that work with victims, especially victims of gun crimes, and they mention that people who were on the gang database were then in turn ineligible for resources.

CHIEF PRIVACY OFFICER FITZPATRICK: So, thank you for that context. I'm not familiar with the particular circumstances that you're describing, so I can't really speak to them on-- speak to that on a direct level. Though, I'm certainly happy to, you

know, engage further, and bring that back for further conversation within the APO universe concerned. You know, this is an area for us where, you know, we've integrated, and it's an academic concept within, you know, the privacy universe, but it's a concept known as contextual integrity, and the idea there, it's-- you know, again, it's an academic framework, but what it boils down to is distilling out whether or not folks would be surprised to learn that their information has been handled in a particular way, given the context of the actors and the activities in question. That's been an element of privacy policy since 2023, I believe. We've endeavored to build on that with our development of a privacy impact assessment which has been an element of our APO toolkit since 20-- since our January 25 update.

CHAIRPERSON WILLIAMS: Okay. Thank you. Yes, I would love to engage further, because I don't even think I realized that there might be some discrepancies by way of our privacy law. Okay. So, do you or the APOs work with the Mayor's Office of Equity and Racial Justice in ensuring equitable approaches to data? If so, can you please describe what the cooperation looks like? If not, is this

something that your office has considered implementing?

CHIEF PRIVACY OFFICER FITZPATRICK: So, I think we have maintained an initiative-by-initiative engagement. I'd have to refresh on what our most recent one is, but you know, we've endeavored to maintain strong relationships, you know, not just across the city's ecosystem, but certainly to socialize the importance of privacy protection, you know, within the Mayor's Office universe of offices, recognizing they're very often on the front line to supporting issue spotting which is a primary objective of ours in support of that, you know, we have a specialized training that we've been doing for that universe of folks for the last, you know, about year, year-plus which we refer to as Privacy 15's. We re-endeavor to distill out the broader universe of training that we would provide and is available within the DCAS catalog into targeted segments that are really tailored from a functional perspective to the sorts of issues that the folks at City Hall encounter. Again, in support of that issue identification where they stop, they think about privacy protection. They think hey, this might be

something, and they understand, you know, who the universe of folks that they should reach out to under any given circumstance, inclusive of my office.

CHAIRPERSON WILLIAMS: Okay. The context for this question is a lot, so bear with me. As you know, the Commission on Racial Equity, CORE, is a new agency established under the Charter in late 2023 that is intended to hold city government accountable for improving equity for all New Yorkers. As a part of this mandate, CORE develops community equity priorities that are intended to serve as a guide for the City to address the most urgent equity concerns of New Yorkers. The number five priority in their inaugural list of equity priorities urges the city to check for and remove any formulas and computer processes that might be biased based on race, ethnicity, or poverty, because these processes contribute to inequities in health care, housing, policing, criminal justice, employment, social service, and more. First, are you familiar with the community equity priorities, and is this something your office has reviewed?

CHIEF PRIVACY OFFICER FITZPATRICK: So, thank you for that context, Chair.

CHAIRPERSON WILLIAMS: [inaudible]

CHIEF PRIVACY OFFICER FITZPATRICK: I'll do my best. You know, it's very-- I'll celebrate CORE. You know, after their formal stand-up as an office, you know, I think we were among the earliest stops among their leadership to get current on, you know, what's the latest and greatest from a privacy protection perspective. We've, you know, engaged with them, I think periodically on initiatives for, you know, requested consultations, and then I'll also celebrate that they were interested engagement with a program that we're really proud of at the Office of Information Privacy which is a citywide privacy legal intern matching programs. You know, we've as an office, got-- increased certainly the number of interested law students who would like t spend a summer with us, and you know, we've got a finite number of positions that we can bring folks onto. And so kind of on-the-fly, but we've done it now for a couple of years, and we look forward to growing it. in the summer of 26. It's still facilitated connections with interested agencies and their privacy officers who'd like to take on a privacy legal intern for summer, and we facilitate

connections, and CORE waws on our inaugural matching program list.

CHAIRPERSON WILLIAMS: I have more, but I'll leave you alone.

CHAIRPERSON GUTIÉRREZ: Okay, we'll come back. Okay, great. Thank you so much. I want to just dig a little bit into some of the policies for the APOs. Each agency must provide-- must have its own privacy policy and your toolkit provides templates. Do you review and approve these agency privacy policies?

CHIEF PRIVACY OFFICER FITZPATRICK: We don't approve. To the extent that we review them, it would be in a posture where we're asked to consult on--

CHAIRPERSON GUTIÉRREZ: [interposing] Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: a policy that's being developed at an agency.

CHAIRPERSON GUTIÉRREZ: And so you don't-- okay. So, they can put together a privacy policy. Are you required-- are you required to review every agency's privacy policy?

CHIEF PRIVACY OFFICER FITZPATRICK: Not at the time of development.

CHAIRPERSON GUTIÉRREZ: Oh, no, okay.

CHIEF PRIVACY OFFICER FITZPATRICK: The mandatory way that that universe of information would pass through would be within the biennial reporting exercise which among required elements includes agency enumeration of their specific privacy policies that they've implemented, and we've evolved our reporting to not just have narrative description of that information, but an ability for agencies to actually attach the policies in question.

CHAIRPERSON GUTIÉRREZ: I'm not sure if I understand that last part. Can you expand a little bit on that? So, just so that I'm understanding, the-- every agency is supposed to have a privacy policy, and you and your teawm don't necessarily review-- do you review every policy?

CHIEF PRIVACY OFFICER FITZPATRICK: No.

CHAIRPERSON GUTIÉRREZ: You don't. You don't have to. It's not mandated.

CHIEF PRIVACY OFFICER FITZPATRICK: No, that's correct.

CHAIRPERSON GUTIÉRREZ: Okay. It's like advisory, it's voluntary for them?

CHIEF PRIVACY OFFICER FITZPATRICK: It's certainly a best practice that we--

CHAIRPERSON GUTIÉRREZ: [interposing] It's a practice.

CHIEF PRIVACY OFFICER FITZPATRICK: That we advise as--

CHAIRPERSON GUTIÉRREZ: [interposing] That's not good.

CHIEF PRIVACY OFFICER FITZPATRICK: As a matter of policy, yep.

CHAIRPERSON GUTIÉRREZ: That makes me nervous. And then I understand you don't approve it, but how do they know this is an acceptable-- this feels like a safe privacy policy. How do you communicate?

CHIEF PRIVACY OFFICER FITZPATRICK: So, that space where we've advised on privacy program specific policies is something that we developed in 2025. Looking at trying our best to help facilitate scaling of privacy best practice within the ecosystem and providing information about, you know, what good looks like for lack of a better term.

CHAIRPERSON GUTIÉRREZ: Do they get a gold star? Like, what-- how does it-- what does it look like?

CHIEF PRIVACY OFFICER FITZPATRICK: That's what our templates-- our templates endeavor to crystalize the source of issues.

CHAIRPERSON GUTIÉRREZ: No, but your templates are very good, but it's advice. It's not mandatory, right?

CHIEF PRIVACY OFFICER FITZPATRICK: That we review privacy policies?

CHAIRPERSON GUTIÉRREZ: That an APO-- yeah, that an APO follows this template to devise their privacy policy.

CHIEF PRIVACY OFFICER FITZPATRICK: That's correct.

CHAIRPERSON GUTIÉRREZ: It's not mandatory. Okay. And do you-- have your reviewed privacy policy?

CHIEF PRIVACY OFFICER FITZPATRICK: We have, yes.

CHAIRPERSON GUTIÉRREZ: Yes, okay. Would you say that you've reviewed them for every agency?

CHIEF PRIVACY OFFICER FITZPATRICK: No.

CHAIRPERSON GUTIÉRREZ: No. Do you-- would say you've reviewed them for the majority of the agency? Or what percentage?

CHIEF PRIVACY OFFICER FITZPATRICK: It would be difficult to come up with a specific percentage, because of course--

CHAIRPERSON GUTIÉRREZ: [interposing] It makes me nervous that there's resource that exists, and they're-- that agencies are opting in to whether or not they want your expert's feedback.

CHIEF PRIVACY OFFICER FITZPATRICK: I-- certainly, I appreciate that perspective, Chair. It's, you know, similar to you know, a point of conversation earlier. That something is an advisory element of privacy policy. It does not mean that that will always be the posture. We're always looking at, you know, whether or not we've got to bring things on the mandatory side of the fence, and we do that, and we think about that, you know, recognizing there are resource challenges, not just on the APO, you know, side of the fence, but you know, certainly within the universe of the Office of Information Privacy. There are limits that nine-- the number of places nine people can be--

CHAIRPERSON GUTIÉRREZ: [interposing] Understood, yeah.

CHIEF PRIVACY OFFICER FITZPATRICK: in any given day.

CHAIRPERSON GUTIÉRREZ: No, no, I understand that perspective. I guess, are there other-- are there other examples, other cities where, you know, there's a Chief Privacy Officer and some of these like privacy policies are voluntarily being shared with the Chief Privacy Officer? I find that concerning.

CHIEF PRIVACY OFFICER FITZPATRICK: Well, our--

CHAIRPERSON GUTIÉRREZ: [interposing] And I totally get the resource, the staffing issue, that's real, but still, nonetheless.

CHIEF PRIVACY OFFICER FITZPATRICK: So, I appreciate the opportunity to actually to talk a little bit about our connections, you know, across the broader municipal privacy community. You know, we've had going back, even before my time, but it's continued and expanded regular conversations with privacy offices across the U.S. Most frequently we're talking with Austin, Texas and Seattle, and

certainly, you know, the feedback that we get about our policies is that we have a degree of maturity as opposed--

CHAIRPERSON GUTIÉRREZ: [interposing] Are theirs voluntary also, or advisory? Excuse me.

CHIEF PRIVACY OFFICER FITZPATRICK: I'd-- I would have to go back and look at their specific postures, but I-- to be clear, the citywide policies are mandatory. What we're talking about is the guidance that we've developed for agencies. If they're developing a particular program or initiative, to have that program and initiative be supported by a privacy policy for that program.

CHAIRPERSON GUTIÉRREZ: Thank you for clarifying. I'm totally clear on that. Nonetheless, I think it doesn't take away from my sentiment of-- I think it's a little inconsistent. I think it's disappointing that it's not-- it's not mandatory, because that coupled with the fact that an APO is assigned by, you know, the agency head that may or may not be consulting with you, that may or may not be looking at these technical criteria, that could really be a recipe for disaster. If you don't have the person with the technical expertise and you don't

have this privacy policy in place that has been, you know, looked at by people that know this language. So that is-- that's-- I understand what you're saying, the distinction that you're making, but I'm trying to elevate that this is a recipe for a lot of violations, and in this climate it makes me very uneasy that sensitive information for folks is at risk and is always at risk, but that like, we're not mandating it at the city level that you all be central to what is approved, what is not approved under this context.

CHIEF PRIVACY OFFICER FITZPATRICK: So, I want to echo that I certainly-- I share your passion for these--

CHAIRPERSON GUTIÉRREZ: [interposing] You're just saying it differently, if you share it.

CHIEF PRIVACY OFFICER FITZPATRICK: I share your passion for these types of issues, Chair. And you know, I agree that we need to continue to build the maturity of our program that allows us to have stronger visibility into these types of practices, particularly recognizing the resource conversations that we've, you know, we've been having. To that end, you know, I've referenced it

earlier, when we've endeavored to build out the reporting structure that's required under the Identifying Information Law every two years. You know, we started from a space where we've evolved from template documents, template Microsoft Word documents that were free text to an environment where we're standardizing the universe of information that we're collecting from agencies, and from there we can have more informed visibility into what's happening. And inherent--

CHAIRPERSON GUTIÉRREZ: [interposing] But they have to opt-in to use it.

CHIEF PRIVACY OFFICER FITZPATRICK: No, biannual reports are required by law.

CHAIRPERSON GUTIÉRREZ: Oh, you're-- I'm sorry. I heard the word template, and I was referring to your toolkit. I understand. Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: The biannual reports are required by law, but there's an inherent dependency within that structure. It's a fantastic thing the Identifying Information Law requires.

CHAIRPERSON GUTIÉRREZ: And the--

CHIEF PRIVACY OFFICER FITZPATRICK: [interposing] Biennial survey of the privacy ecosystem here in New York City, you-- it inherently drives revision, update, and thoughtfulness, but it's dependent on those snapshots every two years.

CHAIRPERSON GUTIÉRREZ: The reporting that you're referring to, this is reporting that every agency has to submit if there were any violation?

CHIEF PRIVACY OFFICER FITZPATRICK: No, this is-- Chair, you're referring to what manifests in the quarterly report from the Chief Privacy Officer. What I'm-- what I'm referring to is the biennial agency reports--

CHAIRPERSON GUTIÉRREZ: [interposing] Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: that are required under the Local Law that have to among other things identify the universe of data elements that agencies are collecting or disclosing and the specific privacy policies in addition to the ident-- to the citywide privacy policies that they're using. That dependency is that information's only coming in every two years. Over the course of the last year

plus, our office has been working to develop requirements for a governance system to-- that APOs can use to do their work to allow them to be more efficient and also have visibility of our office into agency practices. That's not limited to two-year snapshots in time.

CHAIRPERSON GUTIÉRREZ: Okay. Okay. Thank you. For the privacy policies in the instances where you and your team are reviewing them, are you-- do you request revisions?

CHIEF PRIVACY OFFICER FITZPATRICK: We have.

CHAIRPERSON GUTIÉRREZ: You do, okay. And do you have a system to check whether the agencies are integrating those revisions, or is it kind of like these are suggestions and-- we hope they do it.

CHIEF PRIVACY OFFICER FITZPATRICK: If we're--

CHAIRPERSON GUTIÉRREZ: We hope they do it.

CHIEF PRIVACY OFFICER FITZPATRICK: I appreciate that question, Chair. In my experience, you know, when we're consulted, it's consulted

meaningfully and so, you know, we're engaged. We've got visibility into that conversation, and you know, we're seeing work product which is inherently collaborative, you know, result down to its final form. You know, it's-- we're not sending comments out and not seeing, you know, what that final product looks like.

CHAIRPERSON GUTIÉRREZ: You're not seeing that, or you are?

CHIEF PRIVACY OFFICER FITZPATRICK: We are.

CHAIRPERSON GUTIÉRREZ: Okay. Okay. And how are you able to see? Are you-- like, how re you able to see that they're making those changes to their policies?

CHIEF PRIVACY OFFICER FITZPATRICK: Well, this would be, you know--

CHAIRPERSON GUTIÉRREZ: [interposing] Part of the reporting?

CHIEF PRIVACY OFFICER FITZPATRICK: groups-- well, it would be, you know-- you've got a universe of folks convening on development of-- you're working on a particular initiative who might reach out for a consultation in a space of, you know,

what a privacy policy should look like. And from there, you know, we're engaged along with, you know, whatever agency partners and stakeholders need to be a part of that conversation. We're asking the sorts of questions that, you know, we've been talking about here. You know, we're providing that feedback and then, you know, when pens are down, you know, that final product is socialized among the universe of folks who are engaged.

CHAIRPERSON GUTIÉRREZ: Okay, okay. Alright. And then, do you-- are there agencies to your knowledge that do not written privacy policies in place?

CHIEF PRIVACY OFFICER FITZPATRICK: No, not to my knowledge.

CHAIRPERSON GUTIÉRREZ: No. Would you be able to share maybe at a later time the amount of agencies that you've reviewed the privacy policies for? Just the number.

CHIEF PRIVACY OFFICER FITZPATRICK: I can certainly go back to-- and it's part of, you know--

CHAIRPERSON GUTIÉRREZ: [interposing] Yeah, of the 126.

CHIEF PRIVACY OFFICER FITZPATRICK: I've celebrated them, you know, over the course of this hearing, but it's our non-attorney staff who have really developed--

CHAIRPERSON GUTIÉRREZ: [interposing] I don't think you're the one reviewing every single-- I think it's you and your team.

CHIEF PRIVACY OFFICER FITZPATRICK: Well, I was referring to the ability of kind of managing our caseload and having better visibility into where we've been spending our time. So, you know, certainly happy to go back and look at what we've got on our side of how many times we've been engaged on those sorts of issues.

CHAIRPERSON GUTIÉRREZ: I mean, how often is an agency updating their privacy policy? There's no like-- there's no specific mandate for that, correct?

CHIEF PRIVACY OFFICER FITZPATRICK: I think we-- we certainly, and I would want to refresh on that, but I thik we do call for, you know, an update and an assessment, you know.

CHAIRPERSON GUTIÉRREZ: How often?

CHIEF PRIVACY OFFICER FITZPATRICK: I think at least annually.

CHAIRPERSON GUTIÉRREZ: Annually, okay. but right now there's no mandate saying it's got to be every six months or even mandating that it has to be every year.

CHIEF PRIVACY OFFICER FITZPATRICK: I think that's certainly how we've advised historically is taking a look, you know, annually and/or is there a material change to the operation of the program, right? If something is changing, you know, that needs to-- that should be driving updates.

CHAIRPERSON GUTIÉRREZ: Yeah, okay. Thank you. My next question is on APO guidances. I know it's part of Local Law 245 from 2017. The Privacy Officer of each city agency should issue guidance to city agency employees, contractors, subcontractors regarding that agency's collection, retention, and disclosure of identifying information. Do you review that guidance as well?

CHIEF PRIVACY OFFICER FITZPATRICK: That are issued by the--

CHAIRPERSON GUTIÉRREZ: [interposing] The APO for every agency.

CHIEF PRIVACY OFFICER FITZPATRICK: The agencies?

CHAIRPERSON GUTIÉRREZ: Yeah.

CHIEF PRIVACY OFFICER FITZPATRICK: Only if we're consulted.

CHAIRPERSON GUTIÉRREZ: Only if they ask, okay. So, this is-- I mean--

CHIEF PRIVACY OFFICER FITZPATRICK: [interposing] Sorry, Chair, I just want to make sure that we're aligned, you know, in our conversation about citywide privacy policy. The privacy-- the citywide privacy policies, those are mandatory, and so when we're distilling that information out in our biennial reports, agencies can identify that as they're following the citywide privacy policies and any additional policies that they have to support privacy practices.

CHAIRPERSON GUTIÉRREZ: Right. They can do-- I think it's that, that they can provide their own guidance on top of the citywide privacy policy which is the mandate which is the law. They can issue-- they should issue guidance to their employees, contractors, subcontractors regarding their collection, retention and disclosure of

identifying information. So, that's why I was asking specific to those guidances. Are there instances where you are reviewing them? I know it sounds like they have to opt-- they have to basically ask you to review those guidances. Are there instances where you have reviewed their specific agency guidances?

CHIEF PRIVACY OFFICER FITZPATRICK: I would want to go back and refresh my recollection.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: There are not circumstances that are immediately coming to mind, but I would want to double-check on that.

CHAIRPERSON GUTIÉRREZ: Okay, okay. maybe you can shed some light in the context of the citywide privacy policy. What information-- what personal identifying information do contractors and subcontractors have-- what could have that information because they have access to it.

CHIEF PRIVACY OFFICER FITZPATRICK: It should be limited to the function that they're providing, the service that they're providing, and carry privacy officer approval to receive it.

CHAIRPERSON GUTIÉRREZ: Okay, and as far agencies-- I mean, every agency is working with a

contractor and a subcontractor. This guidance that you're going to get back to me on, you're not sure if-- you're not sure necessarily what the guidance that they are sharing with a subcontractor is outlining with regards to personal information?

CHIEF PRIVACY OFFICER FITZPATRICK: So, thank you for that, Chair. You know, agencies, of course, they can build on top of, but as we've talking about, you know, we endeavor to try to make in-scale privacy protection in a number of different ways, and that includes-- you know, within the toolkit, for example, we've got a primer on Identifying Information Law, for example. That exists so that way agencies can take it off the shelf and have a product that we've prepared very much intentionally as an office to socialize among folks that they may be engaging with about what does the Identifying Information Law do, and what does it mean to them. And from a contracting perspective, you know, we've been talking about that issue spotting, that work that we do. You know, it's-- we can't be everywhere that-- at once, but we can establish partnerships and make sure folks are aware of, you know, the core requirements that are necessary from a

privacy protection perspective, and we're actually really excited about partnering with the Mayor's Office of Contract Services for a webinar next month in celebration of our Data Privacy Day programming.

CHAIRPERSON GUTIÉRREZ: Oh, there's a whole day.

CHIEF PRIVACY OFFICER FITZPATRICK: There's a whole day, January 28th.

CHAIRPERSON GUTIÉRREZ: Parade time.

CHIEF PRIVACY OFFICER FITZPATRICK: Every year.

CHAIRPERSON GUTIÉRREZ: Okay. That's wonderful. Okay. So, I get-- so I am-- I know you understand what I'm saying. So, I think the extreme scenario where there is an APO that's been designated that doesn't have-- that doesn't necessarily meet kind of the criteria that you look for when you're asked to weigh in, right? Experience, interests-- in the instance where this APO has been designated doesn't have that in the instance where the privacy policy hasn't been reviewed in the instance where specific guidances haven't been reviewed, there are going to be potentially these like terrible scenarios. In my-- my line of questioning is to

understand how you can make an agency do the right thing. How can agencies have a better process, better uniformity with how they communicate with you, how they designate these folks. Yes, it is resources, but I'm concerned that there's a lot of holes here and there's not a lot of consistency. And as we know, every agency is in desperate need of these privacy policies. Every agency is working more and more with New Yorker's personal information as well as their own employees. So, I'm trying to avoid this worst case scenario, but what I'm hearing is a lot of holes, and so what do we need to do in this next administration? What do we need to do to tie that all in, and to make some of these thing mandatory so that your team of experts are reviewing privacy policies so that you are approving in a sense of these policies, so that you are weighing in on APO designations, and so that you are weighing in on guidance. I'm concerned. I'm concerned, and I'm-- you know, there are agencies that don't have to do this. That's what I'm trying to get from you. What do we need to do?

CHIEF PRIVACY OFFICER FITZPATRICK: Absolutely Chari, and as I indicated earlier, you

know, I share your passion for these issues. And I welcome the opportunity to further engage with the Council on how we can continue to drive that maturing, elevate, and invest in the program, and drive that accountability through all of, you know, the verticals that, you know, exist as well as establish appropriate new ones that might be necessary within the city's, you know, ecosystem. You know, I can share, you know, some of the other work streams that we're engaged in, you know, selling into that point. And when we think about program resiliency, you know, as we've talked about it, not everybody necessarily has, you know, certifications like the folks in my office holds, and you know, we can have attrition that can manifest at any time within the APO network. So, one of the things that we're currently working on as an office is evaluating the development of a citywide contracting services where we can bring on, at least even on a temporary basis, somebody with the relevant privacy expertise who can plug into that APO role in the event that the agency does not have a bench that they can call upon. Similarly, you know, when we-- you know, we've been talking about how can we provide that support when

things don't go according to plan. We're working on that same type of resource, that tool in our toolbox in the audit space where if we're-- find ourselves in an environment where we're responding to a circumstance that requires a technical expertise to go under the hood of how a particular vendor has been doing business, you know, through the lens of what they've agreed to contractually, you know, we've got some external resources that we can call upon under those circumstances to drive that accountability.

CHAIRPERSON GUTIÉRREZ: Okay, thank you. I think I've-- we've both emphasized this. I'm going to just shift gears very quickly. [inaudible] I know that in the Local Law 245 there are requirements for city agencies to follow in the event of a breech of PII. There's a form for New Yorkers to file a complaint in the event that personally identifying ifnormaiton has been collected or disclosed. Can you share how many complaints if any you have received? In 2023, I think your-- when you testified you said there was one.

CHIEF PRIVACY OFFICER FITZPATRICK: I don't know that we've received one this calendar year, but I'm happy to go back and double-check.

CHAIRPERSON GUTIÉRREZ: Can you confirm? And then what about 2024?

CHIEF PRIVACY OFFICER FITZPATRICK: I'd also have to do that same-- that same confirmation. But I don't-- complaints, none are coming to mind--

CHAIRPERSON GUTIÉRREZ: [interposing] None? Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: as I sit here.

CHAIRPERSON GUTIÉRREZ: Okay. How many--

CHIEF PRIVACY OFFICER FITZPATRICK: [interposing] Now caveat, public complaints, right?

CHAIRPERSON GUTIÉRREZ: Yes.

CHIEF PRIVACY OFFICER FITZPATRICK: Like, there's--

CHAIRPERSON GUTIÉRREZ: [interposing] That's right. That every New Yorker has the ability to put that complaint in, exactly.

CHIEF PRIVACY OFFICER FITZPATRICK: Yes.

CHAIRPERSON GUTIÉRREZ: Okay. Does your office conduct independent audits of how agencies handle personal data?

CHIEF PRIVACY OFFICER FITZPATRICK: We do not.

CHAIRPERSON GUTIÉRREZ: And it doesn't need to be like real-time monitoring.

CHIEF PRIVACY OFFICER FITZPATRICK: As I understand the question, I think, Chair, this goes to that auditing resource that I was describing earlier. You know, we've-- audit capability is a dedicated, you know, practice area, and to do it appropriately, you've got to have the right kinds of personnel and resources involved in that process. You know, that-- that is not the operating posture that we have currently.

CHAIRPERSON GUTIÉRREZ: Do you-- do you have the ability to audit at least under-reporting disclosures?

CHIEF PRIVACY OFFICER FITZPATRICK: Is there under--

CHAIRPERSON GUTIÉRREZ: [interposing] But not like day-to-day auditing. But in the event that an agency is disclosing a violation, are you then able to look at that report and then see is this all of it? Like how-- I'm just trying to see how much you all can dig into these violations with every agency and specific with handling violations of personal data.

CHIEF PRIVACY OFFICER FITZPATRICK: Understood. Thank you for that clarification, Chair. That's part of our due diligence when we receive notifications that are required of us from agencies pursuant to policy. That's supposed to happen within 24 hours of discovery. When I talk about, you know, the efforts that we've done over the course of the last few years to drive the maturity of the program, you know, that includes standardizing, you know, the narratives associated with, you know, the types of circumstance that we're seeing, so that way that we can conduct appropriate training of the APO community on here-- here are the circumstances that are seeing most frequently so that way they understand that there's a privacy nexus and can be on the lookout for those types of circumstances.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: At the agency level.

CHAIRPERSON GUTIÉRREZ: How do you-- and I'm so sorry to ask you to repeat yourself. How is that you're able to-- how do you do that? How do you approach agencies to have those conversations?

CHIEF PRIVACY OFFICER FITZPATRICK: We have a dedicated form that we've established known as an Identifying information Law notification Which all agency privacy officers must use when they become aware that identifying information's been disclosed without their authorization.

CHAIRPERSON GUTIÉRREZ: They have to use it. They have to--

CHIEF PRIVACY OFFICER FITZPATRICK: [interposing] Yes.

CHAIRPERSON GUTIÉRREZ: This is part, okay.

CHIEF PRIVACY OFFICER FITZPATRICK: They have to. Even if we recognized circumstances can move quickly, we want to know.

CHAIRPERSON GUTIÉRREZ: Of course.

CHIEF PRIVACY OFFICER FITZPATRICK: So, if they have to send an email, eventually we'll still have to send it for them [sic].

CHAIRPERSON GUTIÉRREZ: Sure. I got you.

CHIEF PRIVACY OFFICER FITZPATRICK: And we do that, because on our side we have a companion part of that notification where we run through entire fact pattern with the Agency Privacy Officer endeavoring

to distill out the kinds of considerations that you would want to or expect to distill out. You know, the types of data elements concerned, you know, scope, etcetera, and that's part of the due diligence where, you know, we're developing a factual record to inform the determination whether or not a reportable event has occurred.

CHAIRPERSON GUTIÉRREZ: And that forum comes to you from the APO?

CHIEF PRIVACY OFFICER FITZPATRICK: Correct.

CHAIRPERSON GUTIÉRREZ: Okay. And then what-- can the APO then make the determination of whether or not this was an improper disclosure or--

CHIEF PRIVACY OFFICER FITZPATRICK: That determination is a Chief Privacy Officer determination.

CHAIRPERSON GUTIÉRREZ: That's your determination, okay. And have you had to make that determination?

CHIEF PRIVACY OFFICER FITZPATRICK: Yes.

CHAIRPERSON GUTIÉRREZ: Yes, okay. okay. and then if an agency chooses not to report a breach, what is the mechanism to catch that. This is-- I

know this is asking for like how do you catch something that you didn't even know happened. How does that-- what does that look like?

CHIEF PRIVACY OFFICER FITZPATRICK: So, it's part of that maturity work that we've talking about this afternoon, Chair, that we're really excited about, and it's those non-attorney staff on our team who are building that framework. You know, translating those ILL notifications in furtherance of developing metrics that can inform better decision-making from a Chief Privacy Officer in that space, and that includes something as simple as identifying when we have not heard from an agency for a period of time. We recognize that this is a world where-- and then like in life, no one is perfect. So to the extent that we're not hearing from an agency for a prolonged period of time, that's a flag up for us where we can drive proactive engagement with the Agency Privacy Officer to get an understanding about, you know, what's going on, what are their policies for notifying and engagement on the agency level, so that way we can make sure that they've got the right kind of visibility. Similarly, you know, that's where, you know, I've been talking about kind of that

targeted training that we're developing, and we look forward to launching early in 2026. It's, you know, those common fact patterns that we're seeing as an office and socializing and walking APOs through them from a table-top perspective, you know, ranging from the simple, the misdirected email. I had a PDF file containing identifying information and I sent it to the wrong Michael Fitzpatrick through the complex which is agency's experience to security incident that involves identifying information. Making sure that our APOs are comfortable enough to operate in that space if and when the time comes.

CHAIRPERSON GUTIÉRREZ: Thank you. I have two more questions and then I'll pass it to the Chair. I have a question about MOUs eventually,interagency MOUs, but I want to get a sense. I know that under previous administrations, the OIP played a leading role in drafting and mediating interagency data sharing agreements, especially around vulnerable populations, like sharing information to identify people who might need assistance during emergencies. Does this interagency agreement-- or interagency agreements, do they still-- do they still exist?

CHIEF PRIVACY OFFICER FITZPATRICK: We are called upon for consulting services in that particular space, Chair. You know, I think a lot of that, our offices had a few different homes since it was founded. We started in the Office of Operations. We moved to the Office of Chief Counsel, and then under this administration we've been part of the Office of Technology and Innovation. But we've continued to engage on those sorts of issues. For example, the Mayor's emergency Executive Order in the context of organizing the city's broader asylum-seeker response, named intentionally so the Chief Privacy Officer as a role to play in that space, and that manifested in us helping, you know, the operational professionals in their work of developing that governance ecosystem, you know, building the plane while you're flying the plane, and that included the development of necessary data sharing agreements to support the city's response.

CHAIRPERSON GUTIÉRREZ: When was the last time that you and your team were brought in to help draft or mediate this, like, interagency data sharing agreement? This year?

CHIEF PRIVACY OFFICER FITZPATRICK: I think we've got a couple pending right now with us.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: It's-- I would characterize it as a regular work stream that we're encountered for--

CHAIRPERSON GUTIÉRREZ: [interposing] Okay, and these are-- and just so I'm using the same language, this is a data sharing agreement or an MO-- data sharing MOU, okay. And have any of these MOU expired in the last three and a half years? Are there agencies sharing data operating without an MOU at this point that you've not reviewed?

CHIEF PRIVACY OFFICER FITZPATRICK: There are certainly MOUs that exist that don't cross the Chief Privacy Officer's desk.

CHAIRPERSON GUTIÉRREZ: I was thinking to like just ones that are particular to data sharing, which that I assume do those-- do all of-- any agreement related to data sharing?

CHIEF PRIVACY OFFICER FITZPATRICK: Not all.

CHAIRPERSON GUTIÉRREZ: No, not all MOU or agreement related to data sharing. What would

qualify an agreement that doesn't come across your desk related to data sharing? Is it something they opt-in to as well, or?

CHIEF PRIVACY OFFICER FITZPATRICK: So, if I'm understanding the question, Chair, that would be an environment that's dependent on us being engaged for consulting services. So, that's, you know, advisory services, and that's not something that-- yeah, it's not something that is-- not a mandatory stop along the way, but it's why we, you know, certainly socialize, endeavor to support, you know, awareness of the office that we do because of who we are and what we do, because we are a value add I think to any conversation that we're a part of, and that includes maintaining strong relationships with the Law Department, recognizing they are a road along the way, and you know, the data sharing MOU space for the administration and often they are folks who reach out to us, you know, to plug us in an particular--

CHAIRPERSON GUTIÉRREZ: [interposing] But it was not the case in previous administrations where it had to-- or any of these agreements or MOUs had to be reviewed by OIP?

CHIEF PRIVACY OFFICER FITZPATRICK: Not to my knowledge.

CHAIRPERSON GUTIÉRREZ: No? Okay. I thought it-- I believe that that's the information that we have. Are there offices now that are working on an interagency agreement to your knowledge that you're not involved in?

CHIEF PRIVACY OFFICER FITZPATRICK: It's hard to know what I'm not involved in. I would suspect so, just by virtue of how big the city's enterprise is, but you know, that's nothing but speculation at my point.

CHAIRPERSON GUTIÉRREZ: Okay. Have there been instances where your-- you or your team have been asked to review a data sharing agreement and you were not able to do that?

CHIEF PRIVACY OFFICER FITZPATRICK: No. If we're asked, we-- we're in.

CHAIRPERSON GUTIÉRREZ: Okay. So, to your knowledge, that's never-- that's never happened.

CHIEF PRIVACY OFFICER FITZPATRICK: Not to my knowledge.

CHAIRPERSON GUTIÉRREZ: Okay. Have you ever had to hold off on being able to review an agreement?

CHIEF PRIVACY OFFICER FITZPATRICK: Hold off?

CHAIRPERSON GUTIÉRREZ: Yeah, I mean, just like-- not like you're reviewing other agreements. Is there like a priority decision tree that you all work on? Like, are there instances where you're being asked to review an agreement, weigh in on an agreement and you're not able to-- and you've not been able to?

CHIEF PRIVACY OFFICER FITZPATRICK: If we're asked, I'm unaware of the circumstance where we have not provided an opinion.

CHAIRPERSON GUTIÉRREZ: Okay. Okay. I know my colleague wants to ask some questions, and then I think I have to read a statement from Council Member Louis.

CHAIRPERSON WILLIAMS: Hi. I have questions about contractors, current contractors. I was a lobbyist at a time and LINC NYC was a client, and I remember that the Police Department was requesting that LINC NYC shared data, their camera

data, because they're like literally big brother with their cameras in New York City, but that's a whole another conversation. But does your office-- I just want any updates. Like, does your office review and approve LINC NYC privacy policy data? And are you aware of, like, any city agencies that currently have access to the data that LINK NYC collects?

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you for that question, Chair. Our office has not had a role with respect to LINC. That's a franchise relationship that's managed with others within OTI. Though certainly, you know, if there are-- it is information that-- folks information is not being used appropriately, that's information certainly that I would like to know about, but I'm-- sorry.

CHAIRPERSON WILLIAMS: Yeah. No. They-- I remember they asked, they requested for the data to be shared. LINC NYC I don't think ever shared it. this was like years ago.

CHIEF PRIVACY OFFICER FITZPATRICK: Okay.

CHAIRPERSON WILLIAMS: So, you know, the program is a little bit more mature now, and so I was just wondering if your office is aware and how that

data may or may not be used within city agencies that LINC NYC is collecting.

CHIEF PRIVACY OFFICER FITZPATRICK: Understood.

CHAIRPERSON WILLIAMS: Because I know ACLU was like not feeling that, of course, but I just again was wondering if your office had any insight around the data that they're collecting and how it may be being used by them and/or city agencies.

CHIEF PRIVACY OFFICER FITZPATRICK: Understood. Our office has not had historic engagement related to, you know, the operation of LINC. I'm certainly aware that there was a privacy audit, an audit, rather, of among other things LINC's privacy policy. And I'm not aware of any deficiencies that were identified that were not addressed.

CHAIRPERSON WILLIAMS: Yep. And speaking of the audit that was done by KPMG, have you all audited any other contractors in similar fashion?

CHIEF PRIVACY OFFICER FITZPATRICK: Not to my knowledge.

CHAIRPERSON WILLIAMS: Okay. Well, it says that your office was involved in the contract

for Altice [sic] for the Big Apple contract, and so if you could share if any of their practices or their-- apparently, according to change order number five, that they are allowed to collect and disclose extensive data such as third party website traffic app usage, browser data, device IDs and television viewing information. So, are-- does this practice comply with New York City privacy protocols?

CHIEF PRIVACY OFFICER FITZPATRICK: So, Chair, thank you for raising this issue. Just to clarify, my office has not had engagement with respect to Big Apple Connect.

CHAIRPERSON WILLIAMS: Are you aware of any privacy protocols and/or potential violations of said privacy protocols?

CHIEF PRIVACY OFFICER FITZPATRICK: It's certainly my understanding that there was discussion of Big Apple Connect, I want to say in September.

CHAIRPERSON GUTIÉRREZ: [inaudible] hearing on it.

CHAIRPERSON WILLIAMS: Oh, your hearing.

CHAIRPERSON GUTIÉRREZ: Yeah, [inaudible]

CHAIRPERSON WILLIAMS: Oh, I'm not on this committee, so I missed it.

CHAIRPERSON GUTIÉRREZ: No, that's okay. Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: And-- apologies, Chair. I believe there's been further questions sent to OTI and others surrounding Big Apple Connect that we received just this morning, and I know folks are working on marshaling that information.

CHAIRPERSON WILLIAMS: Okay. And now I'm turning attention to sharing data with federal law enforcement agencies. So, do you believe New York City agencies should be allowed to share resident data with federal law enforcement? If so, under what circumstances if any?

CHIEF PRIVACY OFFICER FITZPATRICK: So, thank you for that question, Chair. The Identifying Information Law is clear in this respect in limiting the universe of information sharing that agencies can engage in to, as I mentioned earlier, circumstances where law requires it. There is a determination that it is in furthernece of ht mission and purpose of the agency or with the consent of the individual.

CHAIRPERSON WILLIAMS: And just-- you are a very experienced person. So, in your experienced

opinion, do you think there are any additional safeguards we should be thinking about that should be in place to prevent any misuse of resident data by federal agencies and/or city agencies?

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you for that particular question, Chair. The public has such a critical role to play in the space of privacy protection. It is a core motivation why we've opened up the ability to receive public feedback on both our policies and our toolkit, as well as why we've instantiated the requirement for having a public-facing mechanism for agencies to receive complaints that can be routed to the Agency Privacy Officer. We want to make sure not only that privacy policies are being followed, we want to have visibility and awareness if folks feel that they're not being followed, so that way we can consider and certainly that I can consider as Chief Privacy Officer what further policy updates might be necessary under our given circumstance.

CHAIRPERSON WILLIAMS: Thank you. I think I am adding my enthusiasm around standardizing when it's happening at agencies. I know some of the briefing documents that we have detailed instances of

breaches and/or maybe misuse of data, and you know, if a lot of stuff is happening at the agency level and they don't necessarily need ot coordinate with your office, I for sure can see how that might be problematic for the city at large. So, I just wanted to say that. Thank you.

CHIEF PRIVACY OFFICER FITZPATRICK: Understood, Chair, and certainly there should be no sunlight, and from my perspective there is no sunlight as a matter of policy. If there are circumstance where identifying information has been disclosed in a way that has not received privacy officer approval, while policy is clear, those circumstances must be reported to me and be reported quickly.

CHAIRPERSON GUTIÉRREZ: Thank you. I just-- before we [inaudible] Council Member Louis' statement, on this about sharing data with federal law enforcement agencies, are you concerned that federal agencies can subpoena data from city agencies or city vendors? And if they have to-- right? If they do subpoena, can you walk us through the process of how the city would provide that data, that requested data?

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you for raising this issue, Chair. It really-- it speaks to the elements of, you know, one of the salient elements of our identifying information rider which is required notice if a vendor receives a third-party request for information from the city that they might be holding, requiring notice to the agency and their designated person by the agency so that way, you know, to the extent--

CHAIRPERSON GUTIÉRREZ: [interposing] They don't have to notify that particular person whose information is being requested of?

CHIEF PRIVACY OFFICER FITZPATRICK: Well, the lens that I'm speaking to it from is-- you know, if we're talking about a circumstance where an agency maintains a contractual relationship with a vendor and that vendor is in receipt of a subpoena and our contracting terms are attached to that agreement, the agency should be notified from the vendor that that third-party request has happened. We do that very intentionally, because we want to make sure that if there are situations where the city wants to, you know, to step in and offer a perspective, you know,

in protection of that information, we've got the visibility to make that informed determination.

CHAIRPERSON GUTIÉRREZ: How many-- okay, thank you. And how many-- have agencies ever requested exceptions to this rider?

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you for raising that, Chair. The requirement that the rider that our privacy protection or rather our identifying information rider not be deviated unless exceptional circumstances exist is a requirement that we put in under this administration. We are very intentional about doing that. We want to make sure that we've got as strong a baseline from a negotiation perspective that these are our contracting terms, but we recognize that sometimes circumstances do require a negotiation, and if those exceptional circumstances exist, we created-- one, they may only be done pursuant to an approval from the Chief Privacy Officer, and--

CHAIRPERSON GUTIÉRREZ: [interposing] From you.

CHIEF PRIVACY OFFICER FITZPATRICK: From me. And two, those circumstances must be distilled out through a structured deviation process that we've

developed to receive that information from folks citywide. We have-- since we've got this deviation process developed, we've received six requests for deviation.

CHAIRPERSON GUTIÉRREZ: Six requests, okay.

CHIEF PRIVACY OFFICER FITZPATRICK: With only two approved, and I think the four withdrawn.

CHAIRPERSON GUTIÉRREZ: Okay. And were any of those-- of the two that were approved, or actually of all of them, were any of them requested from a federal agency?

CHIEF PRIVACY OFFICER FITZPATRICK: No.

CHAIRPERSON GUTIÉRREZ: No, okay. And what is the-- I don't know how much you can share on this like deviation. I'm really am interested in this, like, exceptional circumstance. Like, what-- what is an example of one if you can share? I mean I'm encouraged by that it's-- you've gotten six this year?

CHIEF PRIVACY OFFICER FITZPATRICK: Yeah.

CHAIRPERSON GUTIÉRREZ: And four were withdrawn, two you approved. So, it doesn't seem

like an exceptional amount, but what is-- what are those circumstances?

CHIEF PRIVACY OFFICER FITZPATRICK: Without getting into the particulars of a negotiation or circumstance, we had a circumstance where the deviation request was in the space of one of our auditing terms, and the entity that was being contracted was another city entity, New York City entity.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: And so under those circumstances, you know, there were-- and given the universe of data elements concerned, you know, that-- those auditing terms that I was describing earlier which say, you know, entity must conduct a comprehensive audit every year of its program, and even if something doesn't go according to plan, they've got to do additional steps. You know, that was a space where we engaged and felt comfortable under the circumstances that we could deviate from the standard language that we had provided.

CHAIRPERSON GUTIÉRREZ: Okay. Okay. But to your-- to your knowledge, the exception-- are

agencies operating whether or not you've approved the exceptions to your knowledge? Like, are they still-- are there instances where agencies are not disclosing or asking for an exception? Do you think that they're violating this piece of agreement?

CHIEF PRIVACY OFFICER FITZPATRICK: Understood, Chair, and it's an area, you know, we find ourselves kind of in that posture of how do you, you know, your prove that negative, and that's a space where we do that awareness, issue spotting, and engagement. It is--

CHAIRPERSON GUTIÉRREZ: [interposing] Have you found-- have you found that to be the case?

CHIEF PRIVACY OFFICER FITZPATRICK: Oh, no, I have not, but it's a motivation-driving that webinar participation that we're going to do next month for Data Privacy Day, you know, socializing amongst--

CHAIRPERSON GUTIÉRREZ: [interposing] January 28th, I'm going to put it on my calendar.

CHIEF PRIVACY OFFICER FITZPATRICK: Look for-- it's a big day. A big day on ours as well. But it's a motivation of connecting within that specialized universe of folks within the city's

ecosystem to review those requirements to make sure that they've got that awareness and can facilitate that issue-spotting. They understand the process. They understand the protocol, and we can go from there.

CHAIRPERSON GUTIÉRREZ: Okay, thank you. I'm just going to-- thank you for the answer. I'm going to read a statement from Council Member Louis. As you know, she's a sponsor of Intro 1340. Good afternoon. Thank you, Chair Williams and Chair Gutiérrez, for your leadership in advancing my legislation today. Intro 1340 addresses an urgent challenge with profound implications for equity in the future of work in our city. Artificial intelligence is increasingly used in agency operations from hiring tools to workforce management systems. Yet, many of these tools can replicate or deepen gender bias without rigorous evaluation and transparency. This bill requires DoITT to conduct biannual gendered impact assessments of algorithmic tools used by city agencies. These evaluations must be done in consultation with labor organizations, gender equity experts, and affected communities to determine whether the use of gender related data

contributes to disparate outcomes in hiring, promotion or discipline. The bill also establishes an interagency taskforce to examine how AI-driven systems influence employment conditions including job displacement, changing responsibilities and workforce composition. We need a coordinated approach to prevent gender-based inequities from becoming entrenched in policy. Women, non-binary individuals and gender expansive workers in public service already face longstanding disparities in pay, advancement in leadership representation. If we fail to examine AI's role now, we risk silently reinforcing the inequities we've worked to dismantle. I encourage my colleagues to support Intro 1340 to ensure gender equity remains central to our technological decisions through transparency, accessibility and public oversight. Thank you again. That's from Council Member Louis on her Intro 1340. I want to just jump to-- since we're on the bills, just quickly jump questions about my college, Council Member Salaam's dot.gov domain. I understand from your testimony that this is, you-- something that you agree with, but what are the-- can you give us some of the reasons agencies have chosen not to use the

.gov domain? I understand from your testimony that this is something that you agree with, but what are the-- can give us some of the reasons agencies have chosen not to us the .gov domain.

CHIEF PRIVACY OFFICER FITZPATRICK: So, thank you, Chair. I haven't been involved in the discussions surrounding this particular bill, but I know others within-- others of my colleagues at OTI have been. And I believe we just-- just before the hearing began this afternoon, I think, received some revisions back from the law Department. So, I'm not really in a position to speak to it, because I haven't been engaged, you know, from my perspective.

CHAIRPERSON GUTIÉRREZ: Sure.

CHIEF PRIVACY OFFICER FITZPATRICK: You know, I think the intent of the bill in establishing known places where folks can contact government is certainly, you know, beneficial and advantageous from a privacy protection perspective. Through that known, you create an ecosystem where folks can feel confident that they're entrusting their information to the extent they are to the known entity.

CHAIRPERSON GUTIÉRREZ: Okay. Alright, thank you. I mean, I think the-- certainly, the

sponsor we'll look forward to reviewing any of that feedback. Can you tell me if it's accurate that the cyber security protections and maintenance of .gov domains are handled by the Federal Government?

CHIEF PRIVACY OFFICER FITZPATRICK: I can't speak to those issues.

CHAIRPERSON GUTIÉRREZ: Okay. And for agencies using .org or .com domains, do you know if there are associated costs for securing and maintaining those domains?

CHIEF PRIVACY OFFICER FITZPATRICK: I can't speak to that issue either, though I'm certainly happy to bring that back to my colleagues who are engaged in the conversation.

CHAIRPERSON GUTIÉRREZ: Okay. Thank you. And then I think on the other-- these are the other resolutions for today, yeah. Can you share if you are supportive of the Right to Your Own Image Act or the-- and the Enacting the New York Data Protection Act?

CHIEF PRIVACY OFFICER FITZPATRICK: So, thank you. Thank you, Chair. For each of the resolutions, expressions of-- expressions, you know, from the administration's perspective most

necessarily involve engagement from stakeholders beyond my office, and we do not have such a statement ready to offer today.

CHAIRPERSON GUTIÉRREZ: You don't-- you're not prepared to say if you support it or not?

CHIEF PRIVACY OFFICER FITZPATRICK: Statements on behalf of the administration extend beyond just me, so--

CHAIRPERSON GUTIÉRREZ: [interposing] Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: I'm not prepared to--

CHAIRPERSON GUTIÉRREZ: [interposing] No, no, I was just asking for-- I'm having a little difficulty hearing you. I was just asking for clarity.

CHIEF PRIVACY OFFICER FITZPATRICK: Oh, sorry.

CHAIRPERSON GUTIÉRREZ: My apologies. Okay. Okay. So, pursuant to admin code Title 23 Section 1205, each agency must submit biennial-- that word is so hard-- identifying information report. The reports include information on the type of data collected by each agency. Please tell us what

agencies collect biometric information, including gait recognition, fingerprints, iris scan, facial geometry. Would you know that NYPD uses facial recognition? What other agencies are using these tools?

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you, Chair. We've got that information. Is that in here?

CHAIRPERSON GUTIÉRREZ: I was hoping one of you would come up, yeah. Oh, he's not messing around.

CHAIRPERSON WILLIAMS: I just have one more question.

CHAIRPERSON GUTIÉRREZ: Yeah, of course. [inaudible] yeah, yeah, I'll pass it to you.

CHIEF PRIVACY OFFICER FITZPATRICK: Sorry.

CHAIRPERSON GUTIÉRREZ: No, no, no, you're--

CHIEF PRIVACY OFFICER FITZPATRICK: [interposing] No, so when we've done a review of the data elements reported in our 2024 cycle, and so there are numerous, you know, collections and disclosures of what we would think of as biometric

information happening across the city's ecosystem. Happy to provide kind of an exhaustive list of our office's review of those reports. For example, there's 44 agencies which are-- sorry, rather 66 agencies which collect photographs, for example. So upon on which photograph is capable of serving as a biometric identifier. So we're happy to provide, you know, your office with a breakdown of what we've seen from our review of those reports.

CHAIRPERSON GUTIÉRREZ: Are there -- okay, so you're saying there's many examples within multiple agencies that are--

CHIEF PRIVACY OFFICER FITZPATRICK: [interposing] Correct.

CHAIRPERSON GUTIÉRREZ: using biometric. Can you share in your binder how many agencies are using gait recognition?

CHIEF PRIVACY OFFICER FITZPATRICK: So, going to kind of-- and bringing back the dependency that I mentioned earlier. So, our analysis is based off of our review of the 2024 reports. So, those are moments in time. We're working on trying to evolve from moments in time to something closer--

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: to real time. Our review in 2024 was that four agencies reported disclosure of gait or movement, and five reported collection of that information.

CHAIRPERSON GUTIÉRREZ: Oh, okay. And then can you share if FDNY uses facial recognition?

CHIEF PRIVACY OFFICER FITZPATRICK: I would have to back and look at it, FNDY's 2024 report.

CHAIRPERSON GUTIÉRREZ: It's not in your big binder?

CHIEF PRIVACY OFFICER FITZPATRICK: It'-- there's a 126 of them.

CHAIRPERSON GUTIÉRREZ: Well, FDNY is a big one. Okay. Please do get back to us on us--

CHIEF PRIVACY OFFICER FITZPATRICK: [interposing] Absolutely.

CHAIRPERSON GUTIÉRREZ: on that. Council Member Williams has a question.

CHIEF PRIVACY OFFICER FITZPATRICK: I'll also note that that engagement though necessarily-- you know, can look at the 2024, but because of the important conversation that we're having today and where we need-- you where we're working towards

going. It's also brining that information current, you know, based of this is what we've seen in 2024. You know, are those practice, you know, current as we hit here. On December 8th, 25.

CHAIRPERSON GUTIÉRREZ: Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: And I'll note, you know, we-- next year is a--- the even number of years are big years for us. Those are compliance years for our office to facilitate that biennial agency reporting review. You know, that work will kick off, you know, end of Q1 where we, you know, provide training like we always do to all APOs on what's expected, and under Local Law, those reports are then due for submissions and the-- to the Chief Privacy Officer, to the Mayor and Speaker of the Council by July 31. Our office will do a technical review of each submitted report through the lens of what's required to be submitted under the Identifying Information Law. Are each of those elements manifesting within each submitted agency report? Once those reports pass that quality control review, we make them available to the Citywide Privacy Protection Committee. That committee will deliberate over the course of August, September, and

October in furtherance of developing recommendations on how we can and how the Chief Privacy Officer can and should evolve citywide privacy policy based off of the observations of what agencies have shared. Those recommendations are submitted to, again, the Chief Privacy Officer, Mayor and Speaker of the Council. At that point, the Chief Privacy Officer is on the clock for implementing policy updates within--

CHAIRPERSON GUTIÉRREZ: [interposing] Oh boy.

CHIEF PRIVACY OFFICER FITZPATRICK: 90 days of receiving those recommendations, and our historic practice certainly during my tenure is to have those policy updates coincide with and around Data Privacy Day the following January.

CHAIRPERSON GUTIÉRREZ: Okay. Alright, excellent. Let me pass it to my colleague now.

CHAIRPERSON WILLIAMS: Yeah. You mentioned in your testimony that you are assessing potential operational impacts of designating certain technological information as private for breech notifications. Can you share any examples or share any additional details about this issue?

CHIEF PRIVACY OFFICER FITZPATRICK: Absolutely, Chair, and thank you for the opportunity to address the Council in regard. The question about including technological information within the city's local breech notification law is really driven by, you know, getting better insight into the particular circumstances the update is intended to address. When we look at the existing universe of data element within the bounds of 10501, 10502 that are considered to be private information, there is a risk of harm that's inherent within the disclosure of that particular data element. You know, the most obvious and I think the first is social security number. If that information is out there, there are negative consequences that can follow to the individual. So, it's really understanding and engaging with the Council on kind of what are the motivations behind the proposal, and so that way we can, you know, offer the most informed perspective that we can across the broader universe of stakeholders who are involved of which I am just one.

CHAIRPERSON WILLIAMS: Thank you. I wanted to ask-- let use this example. I hope that you can answer these. This happened I think just a few

months ago. This is the New York City Housing Connect Lottery Portal. It experienced a misconfiguration that exposed applicant names. I mean, it was pretty easy just to like look up any-- just to look it up, and so everyone's live information-- and if anyone here has not applied through Housing Lottery, it's all of your information, your income. It's your family's information, date of birth, where you resided, where you reside, so super, super personal information. And so this was available to anyone searching. Can you share the steps that OTI-- that your office took in response? And I know that there's HPD here involved, and there was the name of the organization, the group, the company that was doing the application. The name is escaping me now. But can you tell me what steps your office took and where did OTI or any other office or agency notify the victims of the folks whose names was compromised?

CHIEF PRIVACY OFFICER FITZPATRICK: So, thank you for raising this particular matter, Chair. I'm certainly aware of it. The lens and there are broader, a broader universe of engagement from folks within OTI, because there's obviously a technical element that goes beyond the responsibilities of my

office. Our lens of engagement was in the space of notification to impacted individuals under those circumstances--

CHAIRPERSON WILLIAMS: [interposing] Your office-- I'm sorry. Did reach out to impacted individuals?

CHIEF PRIVACY OFFICER FITZPATRICK: We supported HPD in affecting notifications--

CHAIRPERSON WILLIAMS: [interposing] Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: to impacted individuals.

CHAIRPERSON WILLIAMS: Okay. Do you have a sense of how many individuals that was?

CHIEF PRIVACY OFFICER FITZPATRICK: I can provide that.

CHAIRPERSON WILLIAMS: Okay. And I guess what steps-- what role did OTI play? Like what steps did your office take after all this information was public?

CHIEF PRIVACY OFFICER FITZPATRICK: So, this is kind of the layered universe, and thank you for that question Chair, in which our office plugs in with other professionals across the technology ecosystem. When you've got a technical matter, you

know, you've got our experts at Cyber Command who are obviously the first responders in that particular space, and certainly we're parts of those conversations as Office of Information Privacy, but the lens in which we come at it is as that factual record is being developed, supporting the identification of data elements concerned with any particular circumstance and assessing whether there's a legal requirement to affect notifications to impacted individuals based on the data elements that are present. And if not, whether it is prudentially advisable to notify those same individuals under a given circumstance.

CHAIRPERSON WILLIAMS: Okay, it's advisable. Are the agency contractors in this instance, this company that was doing the application, are they required to comply with the citywide privacy policy?

CHIEF PRIVACY OFFICER FITZPATRICK: I believe--

CHAIRPERSON WILLIAMS: [interposing] As like a subcontract-- as like a contractor to HPD?

CHIEF PRIVACY OFFICER FITZPATRICK: I believe so.

CHAIRPERSON WILLIAMS: Yes, okay. Okay, and then how can you-- how do ensure compliance?

CHIEF PRIVACY OFFICER FITZPATRICK: So, sorry, Chair, you just-- was your question cyber security policy or privacy policy?

CHAIRPERSON WILLIAMS: Privacy policy.

CHIEF PRIVACY OFFICER FITZPATRICK: The answer remains true. I believe so.

CHAIRPERSON WILLIAMS: Yes, okay. And then how are you able to ensure a compliance?

CHIEF PRIVACY OFFICER FITZPATRICK: With a vendor?

CHAIRPERSON WILLIAMS: With-- yeah, the subcontractor in this example.

CHIEF PRIVACY OFFICER FITZPATRICK: So, that's a circumstance where, you know, the efforts that we've taken with respect to strengthening our privacy contracting terms manifest and specifically reserving the additional rights in the audit space, not just in good times, but when there are bad times that have happened, reserving additional rights for the city to obtain additional information moving forward from vendors concerned.

CHAIRPERSON GUTIÉRREZ: And then on-- just so that I'm all set on the auditing, is this-- are in-- are you-- do you have the capacity to do independent audits? Are you only doing this after reporting is done? How does that look for your team?

CHIEF PRIVACY OFFICER FITZPATRICK: We do not have the standing capacity to affect audits. It's a primary motivation while we're evaluating the development of having an external resource in our toolbox that we could call upon, you know, depending on whichever circumstances that may manifest.

CHAIRPERSON GUTIÉRREZ: Do you think that it is important? Is that something-- is that a direction that you want to go in to be able to have the capacity to do independent audits?

CHIEF PRIVACY OFFICER FITZPATRICK: I believe that it's important to validate, you know, expectations are being met with respect to privacy compliance.

CHAIRPERSON GUTIÉRREZ: So, yes.

CHIEF PRIVACY OFFICER FITZPATRICK: I think it's an important exercise.

CHAIRPERSON GUTIÉRREZ: Okay. Okay. I want to talk about-- I think Council Member Williams

touched on it-- or ask you a series of questions regarding the audit conducted by KPMG regarding data collected for a LINC kiosk. I'm specifically asking about the city's contract with Talk Space which is an online mental health platform provided to all New York City Public School students ages 13 to 18, I believe. It's a $26 million contract. I know earlier this year there was a letter send to all of us and to advocates about student privacy and how parents and advocates felt that was being compromised. Can you share-- following that incident with Talk Space, has your office changed any of its practices regarding the review of vendor data practices and privacy policies?

CHIEF PRIVACY OFFICER FITZPATRICK: So, when we and I think about necessary steps in evolving the city's privacy program, I'm--

CHAIRPERSON GUTIÉRREZ: [interposing] Oh, wait, I'm so sorry to interrupt you. Very quickly. has your office been able to audit Talk Space or considered auditing them since that information became public?

CHIEF PRIVACY OFFICER FITZPATRICK: So, this is a-- understood, Chair. This is an area

where, you know, I want to be careful about, you know, speaking on behalf of another agency. I can share that certainly we were engaged collaboratively with the Health Department.

CHAIRPERSON GUTIÉRREZ: Before the contract was designated, or?

CHIEF PRIVACY OFFICER FITZPATRICK: In response to--

CHAIRPERSON GUTIÉRREZ: [interposing] Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: the letters that you're referring to. And taking a step back, I look to all forms of engagement that we're seeing across the broader ecosystem to think about what additional tools that we need in our toolbox or should have in our toolbox, and certainly that is a fact pattern that has informed the work that we've been doing and htikning about how to develop that external audit resource that agencies could call upon on a given circumstance.

CHAIRPERSON GUTIÉRREZ: So, your-- you are looking for ways to audit, or?

CHIEF PRIVACY OFFICER FITZPATRICK: To secure those resources that--

CHAIRPERSON GUTIÉRREZ: [interposing] Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: could be used by agencies under a given circumstance.

CHAIRPERSON GUTIÉRREZ: Okay. And just my original question, are there ways that your office is changing its practices? I mean, just for context-- and you nodded, so I know that you know this. There was sensitive information being shared that we the city are now suing these social media platforms like TikTok, Meta, and Snap-- or Snapchat, is that what that is? They were using information that when teens were initially logging on which was asking like date of birth, mental health issues, full name, that information was being sold to them. So, how are you all changing-- considering all of that, the gravitude [sic] of all that? How are you all changing your practices when you review these data practices or these privacy policies with vendors or subcontractors? So, absolutely appreciate the question, Chair. The-- I think most saliently is and immediately is the guidance that we've developed within our toolkit and integrated within our policies, flagging that the use of online analytics

require a unique consideration by agency privacy officers, scaling that awareness, you know, downstream within the city's ecosystem.

CHAIRPERSON GUTIÉRREZ: Was this something-- and I'm sorry. Just to clarify for me, was this-- was this something that could have been avoided by the work of an APO, kind of like-- I'm not trying to point fingers, but you know, and I know this is very specific, because as I understand it they were using like tracking pixels-- how could this have been avoided? It's a massive contract, $26 million. Who is-- how do we avoid this? How does this happen? How does-- and I believe the site was live for many months before, you know, before we got the letter from advocates, and by that time, you know, young people's information had already been sold. So who's responsible in an agency when this happens?

CHIEF PRIVACY OFFICER FITZPATRICK: So, from our perspective, it's why we endeavor to scale governance in as many places as we can. It's through that analytics guidance that I referenced earlier. It's why we've identified key personnel and call on key personnel in our policies--

CHAIRPERSON GUTIÉRREZ: [interposing] And I'm sorry. So sorry to interrupt you. This information was sold, to your knowledge, to these social media companies?

CHIEF PRIVACY OFFICER FITZPATRICK: I'm sorry, Chair, I can't speak to that right now. I'd have to go back and engage.

CHAIRPERSON GUTIÉRREZ: Okay. It was shared.

CHIEF PRIVACY OFFICER FITZPATRICK: And follow up.

CHAIRPERSON GUTIÉRREZ: It was shared-- anyway. Okay.

CHIEF PRIVACY OFFICER FITZPATRICK: But to the point of scaling governance, it's why we identify key personnel within the agency-- within agencies that APOs should maintain regular engagements with. It's why we have integrated that online analytics guidance, socializing that these are issues that require special attention.

CHAIRPERSON GUTIÉRREZ: Did that guidance exist before this particular contract was secured?

CHIEF PRIVACY OFFICER FITZPATRICK: I'd have to review the timeline. That guidance was

published as part of our January 2025 policy update, I believe.

CHAIRPERSON GUTIÉRREZ: Okay. Okay. If you can check. I think we can also check to see when the contract was confirmed. I think it was before. Okay, sorry, my apologies. Okay. Can you share what verification if any is required before-- I'm sorry to jump around-- before an agency-- before an APO relies on NYPD's assertion that a disclosure is connected to a criminal investigation?

CHIEF PRIVACY OFFICER FITZPATRICK: Sorry, Chair, can you repeat that?

CHAIRPERSON GUTIÉRREZ: So, this is regarding Agency Privacy Officers who are consulted with respect to disclosures to New York City Police Department should accept the NYPD's assertion that the disclosure is in connection with an investigation of a crime. What-- my question is what verification if any is required before that APO relies on their assertion that the disclosure is in fact connected to a criminal investigation?

CHIEF PRIVACY OFFICER FITZPATRICK: Thank you for that question, Chair. That the information in that representation is coming from an identifiable

member of the NYPD is what we were endeavoring to accomplish with that particular policy update. And endeavor us to do so because we had, as Chair you may be aware, the Identifying Information Law contains an exception surrounding the providing of identifying information from agencies to the Police Department in connection with criminal investigation, and in the inexperience of our office there had been uncertainty among the APO community on how to think about those sorts of issues to the extent that they manifest in their work which was the motivation behind providing that policy clarification.

CHAIRPERSON GUTIÉRREZ: Okay. Okay. I'm going to wrap up the questions with a series of questions regarding the OATH ticket surge. I believe-- I know the letter was sent to your office in October, so we're just going to make sure you have it in front of you now. It's-- I'm going to-- for the following questions I'm going to be referring to a letter that was sent on October 2nd of this year. It's about a sensitive issue and this committee doesn't want to draw attention to it on the record. So, going forward, I'd like us all to refer to the data set as data set X. That agency in question is

agency X. We can give you the letter, too. We have printed that letter for you and it's in front of you. Can you agree to those terms referring to the data set X and agency X?

CHIEF PRIVACY OFFICER FITZPATRICK: I can.

CHAIRPERSON GUTIÉRREZ: Okay, great. Thank you. When did your office first become aware that data set X search system were enabling mass exposure of personal information? And some of this information includes names, date of birth, home address, driver's license number.

CHIEF PRIVACY OFFICER FITZPATRICK: I'm happy to go back and provide a review of the historic engagement with my office.

CHAIRPERSON GUTIÉRREZ: But you don't remember when you first became aware of this?

CHIEF PRIVACY OFFICER FITZPATRICK: No, I'd have to review. I want to be clear. I want to make sure that I'm precise when talking--

CHAIRPERSON GUTIÉRREZ: [interposing] Okay, because I know it's been brought up as far as back as going back to 2019 and then again in our letter in October 2025.

CHIEF PRIVACY OFFICER FITZPATRICK: Which is why I want to be clear about the historic engagement.

CHAIRPERSON GUTIÉRREZ: Okay. Well, you have-- y'all's office has not responded. So, I hope that in the response you'll be able to include that.

CHIEF PRIVACY OFFICER FITZPATRICK: Chair, if I may, the correspondence in question and speak on it. You know, our office has been engaged and continues to be engaged collaboratively with the agency concerned, working towards resolution, and steps forward with respect to the issues identified both in the near, medium and long term, and it is my expectation that, Chair, you and the Council will receive the substantive update that we committed to providing within the timeline that we committed to providing it.

CHAIRPERSON GUTIÉRREZ: Okay. We've got a few weeks left of this administration,--

CHIEF PRIVACY OFFICER FITZPATRICK: [interposing] Understand.

CHAIRPERSON GUTIÉRREZ: so I look forward to that response. Can you just tell-- can you just share with me if you believe any of that information

that I shared that was live includes date of birth, home address, driver's license, phone numbers-- would you classify this as sensitive personal information?

CHIEF PRIVACY OFFICER FITZPATRICK: So, that's-- Chair, I want to be careful about speaking unilaterally when we're engaged in a joint review with respect to the practices. I'm happy to include my assessment of those practices in the joint response between OTI and the agency concerned.

CHAIRPERSON GUTIÉRREZ: You're referring to OATH as the joint--

CHIEF PRIVACY OFFICER FITZPATRICK: [interposing] I wanted to make sure-- I didn't-- I wanted to make sure I wasn't violating the ground rules.

CHAIRPERSON GUTIÉRREZ: I started my question with them. I'm just-- so you're not-- you cannot-- I think in the context of this, the whole purpose of this hearing, we want to make sure that at the very least we're on the same page of what constitutes personal information. So that's-- to me, it is any of that, anything-- your name, your date of birth, your address, your driver's license number.

You cannot tell me if you feel that this is in fact sensitive data.

CHIEF PRIVACY OFFICER FITZPATRICK: Well, I think it's-- as we've been talking about the unit, it certainly constitutes identifying information. Whether or not it constitutes sensitive identifying information is always going to be a context-specific determination. And once again, I'm happy to bring that back and include that as an element of the response. You know, the other element that we have to be also cognizant of is, you know, thinking about how all of that intersects with the Identifying Information Law and agency compliance, and to the extent to which that information, even if identifying, is based upon-- the disclosure of that information is based upon an appropriate Agency Privacy Officer approval. So, these are a broader-- you know, there's a broader universe of considerations that go into answering the question, but I'm happy to bring that back and make sure that there's an element of the response that's provided to you.

CHAIRPERSON GUTIÉRREZ: So, this information that I just listed out, this personal

information, is currently available in two places and via agency X's own systems which they control and Open Data which you control-- which OTI controls, excuse me. Should-- am I-- should I understand that this level of exposure is not sensitive under your own policies. It's still live 'til this morning. We checked this morning.

CHIEF PRIVACY OFFICER FITZPATRICK: We certainly have been working and appreciate the concerns raised and the correspondence that you're describing, Chair. We take them seriously. I take them seriously. It's why we've established an enhanced directors of public engagement with our office and with APOs citywide, and we look forward, and I look forward to--

CHAIRPERSON GUTIÉRREZ: [interposing] But why hasn't that been-- why hasn't that level of access been taking down? Considering-- I understand that you're responding to the letter, and understanding-- I don't know if you're investigating, but it just seems like people's full names, date of birth-- I don't know why you need a driver's license number, but all of that information is like seriously personal, and I think it would jeopardize anyone and

can-- until this day it can be found. So, I just at the very least, this whole context of this hearing is how do we protect people's information. That's something that is under your purview and it's still live and still searchable today.

CHIEF PRIVACY OFFICER FITZPATRICK: The--

CHAIRPERSON GUTIÉRREZ: [interposing] And the letter was October 2nd, dated for October 2nd.

CHIEF PRIVACY OFFICER FITZPATRICK: The-- certainly we come at this issue from a privacy perspective. This is also one, an issue, and I think it manifests across the broader ecosystem, certainly baked right into the foundation of the Identifying Information Law where agencies are making mission and purpose determinations, where the agency concerned being OATH has a position related to its practices. I'm not in a position where I can speak on behalf of OATH, but I am in a position of conveying to you that this is-- you know, if unpacking that decision-making is of importance to you, Chair, to bring that back and make sure that it's a necessary element of our response of which we anticipate to be timely.

CHAIRPERSON GUTIÉRREZ: Okay. I understand you cannot speak for OATH. I'm

disappointed by OATH. You can take this back. They can read the transcripts about their just cavalier response to people's information being live and available, but Open Data is under your purview. Why has it not been curbed so that people's personal information-- in any other data set I believe it's typically redacted. Why under this particular data set is it still live and available?

CHIEF PRIVACY OFFICER FITZPATRICK: So, thank you, Chair, and to provide clarification, my office does not have a responsibility in Open Data implementation.

CHAIRPERSON GUTIÉRREZ: OTI does.

CHIEF PRIVACY OFFICER FITZPATRICK: OTI and then the Office of Data Analysis facilitates that particular program for governance, but similarly, the Open Data related to terminations also necessarily involved determinations that are made at the agency level. And again, OATH certainly, you know, has a perspective to offer in that particular space, and like--

CHAIRPERSON GUTIÉRREZ: [interposing] But don't you have perspective to offer as the Chief Privacy Officer with respect to Open Data? Right

now, I'm just saying, and I'm not-- I could ask you for your name, your driver's license information, your date of birth information. That's information that's live right now. That's your personal information, and you're saying that it lives within Open Data. You're admitting that it lives within Open Data, but that's OTI and that's not you, but you're the Chief Privacy Officer for the city. Shut it down.

CHIEF PRIVACY OFFICER FITZPATRICK: Chair, I certainly appreciate, like I've said several times, your perspective on--

CHAIRPERSON GUTIÉRREZ: [interposing] I'm just not hearing the urgency.

CHIEF PRIVACY OFFICER FITZPATRICK: these issues.

CHAIRPERSON GUTIÉRREZ: At all from you.

CHIEF PRIVACY OFFICER FITZPATRICK: I can-- I can share with you the urgency of the engagement that we're working collaboratively with OATH on the timeline that we're working.

CHAIRPERSON GUTIÉRREZ: What is the timeline if you can share?

CHIEF PRIVACY OFFICER FITZPATRICK: We committed to providing a responsibly within six weeks of our update to you which I believe at six weeks is December 18, approximately. So, there's a response to, you know, certainly within the next 10 days.

CHAIRPERSON GUTIÉRREZ: Okay. And who is the APO for agency X?

CHIEF PRIVACY OFFICER FITZPATRICK: I can provide that information. I also wanted to emphasize, though, you know, I take this seriously. OATH takes this seriously. You know, and the conversations on responding to the correspondence has been conversations that I've been--

CHAIRPERSON GUTIÉRREZ: [interposing] I believe that.

CHIEF PRIVACY OFFICER FITZPATRICK: directly engaged with their Commissioner in regard.

CHAIRPERSON GUTIÉRREZ: I am-- I will be waiting with bated breath for that response by December 18th. I'm saying in the meantime, the fact that so many New Yorkers' information is live. Concerns me that there is not something that you can effectuate right now as the Chief Privacy Officer to say like, yes, we are responding to this letter, and

yes, we're going to investigate. In the meantime we got to take this stuff down, because it is out there for public.

CHIEF PRIVACY OFFICER FITZPATRICK: Understood, Chair, and I'm happy to bring that back. If there are steps that we can take in interim--

CHAIRPERSON GUTIÉRREZ: [interposing] You don't have to take it back. It's to you, directly. You're the Chief Privacy Officer.

CHIEF PRIVACY OFFICER FITZPATRICK: Like I've said, there are agency-related determinations that are necessary elements of that conversation. Those determinations have been made, but I will absolutely share your perspective and facilitate a timely response to you.

CHAIRPERSON GUTIÉRREZ: Okay. I hope that as part of that response, you're-- the-- you're prepared to share what happens if anyone's information has been used and compromised in any way, because it's been live for years, and we sat here on December 8th with the ability to take that information down and didn't. Okay. You got anything else? Prior to this, I want to thank you for everything else. I think-- I look forward to

continuing the conversation. I of course want to be able to codify a lot of what you and your team have been working on and hope that we can get to a point where your team and your unit is empowered to mandate, to follow the toolkit that you all spent so much time on. Thank you. Thank you so much.

CHIEF PRIVACY OFFICER FITZPATRICK: I also, if I may, I said at the top I want to conclude it-- include this important conversation today. I am grateful for the opportunity to share the great work that the Office of Information Privacy has been doing since its inception and the great work that our Agency Privacy Officers have been doing. I certainly appreciate, like I've said, the passion for privacy protection. I share it, and I look forward to continuing to engage with the Council on how we can continue to mature our privacy program in support for all New Yorkers.

CHAIRPERSON GUTIÉRREZ: Yeah, I think a lot of that was in our hearing today. So, thank you. Thank you for your responses and your testimony. I look forward to that response. I now open the hearing for public testimony. I remind members of the public that this is a formal government proceeding and that

decorum shall be observed at all times. As such, members of the public shall remain silent at all times. The witness table is reserved for people who wish to testify. No video recording or photography is allowed from the witness table. Further, members of the public may not present audio or video recordings as testimony, but may submit transcripts of such recordings to the Sergeant at Arms for inclusion in the hearing record. If you wish to speak at today's hearing, please fill out an acceptance-- appearance card, excuse me-- with the Sergeant at Arms and wait to be recognized. When recognized, you'll have three minutes to speak on today's hearing topics, use of surveillance-- no, that's wrong. If you have written a statement or additional written testimony you wish to submit for the record, please provide a copy of that testimony to the Sergeant at Arms. And just to the topic of today's hearing is privacy protection in the digital age. You may also email written testimony to testimony@council.nyc.gov within 72 hours of this hearing. Audio and video recordings will not be accepted. Our first panelists are Clayton Banks, Talia Kamran, and Alissa Johnson. You

can get started with whoever wants to go first, sorry.

CLAYTON BANKS: Hello, everyone. And it's-- I'm just so happy to be here. It's been a long time. I have to say that good afternoon, obviously. It almost feels like night. It's been a long time. Jennifer Gutiérrez, my God, you are an amazing person. I got to tell you. First I met you, you were like 50 percent. Now you're like at 2,000 percent. It was crazy. I love it. I'm sorry. So, at any rate, thank you for the opportunity to speak here. I really do appreciate it, and I do-- I'm very-- privacy protection is something that I'm very much about, and I wanted to talk a little bit about it. We're talking about a lot of the things that are happening out now, right now with the deep fakes and all these types of things going on, and what I want to make sure that we are connecting that to internet at the same time. So, internet and all this stuff that's going on right now is happening, both of them at the same time. So, the way we look at it from our perspective is that for more than a decade in my particular organizations has worked across upper Manhattan to help residents embrace technology,

right? And however, people will only embrace innovation if they trust it. And privacy is not separated from innovation, it is the foundation that makes innovation possible. So, there's so much going on. It's going on right now. So, for us, we without-- to me anyway, without universal internet access, deep fakes become even more dangerous, literally. And when communities in a lot of ways lack fast, reliable, affordable internet, they struggle with outdated information, low digital literacy, inability to check sources, no access to verification tools, delayed alerts about scams or fake videos, less exposure to accurate news, more vulnerability to misinformation-- I'm always wondering if somebody's using my voice, but anyway. Digital inequity magnifies digital harm. A disconnected community becomes an easy target for manipulation, and I know that in Harlem. So, from my perspective, this is something to really keep on your mind. That is why universal internet access must be seen as a civil right in the digital age. That's the way I feel about it. It protects seniors, protects youth, protects families, and protects democracy itself. What communities and elected officials can

do together, support policies that accelerate low-cost and no-cost broadband, that high-speed internet like heat and water,-- is that something?

CHAIRPERSON GUTIÉRREZ: You can just wrap up here.

CLAYTON BANKS: Let me wrap it up then. I have an idea, and I hope you can think of it with me, what I call Digital Rights Zone, a partnership that positions Harlem as a model neighborhood for AI fairness, privacy protections, safe digital infrastructure. We are able to do this. So, I have a lot more around that, but I'm--

CHAIRPERSON GUTIÉRREZ: [interposing] Yeah, let's talk. This sounds really interesting. Do you have a written test--

CLAYTON BANKS: [interposing] I can't wait.

CHAIRPERSON GUTIÉRREZ: Do you want to provide us with your written testimony?

CLAYTON BANKS: I did. I sent it in.

CHAIRPERSON GUTIÉRREZ: Oh, you did, okay.

CLAYTON BANKS: And I'll send more.

CHAIRPERSON GUTIÉRREZ: Okay, excellent.

CLAYTON BANKS: Thank you very much.

CHAIRPERSON GUTIÉRREZ: Thank you. Of course.

ALISSA JOHNSON: Hi. I'm Alissa with the Surveillance Technology Oversight Project. We're a New York-based civil rights and anti-surveillance group that advocates and litigates around discriminatory surveillance. I just want to take some time today to talk about our positions on some of the proposed introductions and resolutions. So, first, Introduction 1335 which is the one about definition of identifying information. STOP's position is that IP and Mac addresses already fall within the definition of Section 231201's information that can be used on its own or with other information to identify and locate an individual. We find that explicitly including these identifiers in the list of identifying information is nevertheless useful for purposes of clarity. So, we support Introduction 1335. Second, with respect to resolution 1062, the Right to Your Own Image Act, STOP has found that right of publicity claims are an important check on data brokers. And strengthening that right can only help New Yorkers and organizations like STOP to hold

data brokers accountable for violating people's rights and therefore STOP supports Resolution 1062. Introduction 1340 about the gendered impact taskforce, we applaud the council's efforts to address the critical issue of gender discrimination and algorithmic decision-making, but we do have concerns that this particular amendment will imperfectly target the issue. We would like to raise the fact that the taskforce currently does not account for algorithms which use close proxies for gender, only gender itself, in compiling a list of algorithms which the taskforce will then review. So, this reporting requirement, we're worried we'll miss algorithmic tools that do discriminate on the basis of gender, but do not explicitly use gender itself as an input. We think establishing a taskforce to ensure that algorithmic tools used especially in hiring do not discriminate on the basis of gender is a laudable goal, but we're worried that such a taskforce would have to analyze all tools used in hiring or in similar topics rather than just those that explicitly categorize gender as an input. With respect to Resolution I think 1783, for the Data Protection Act, STOP actually has some concerns about

the Data Protection Act as it's currently written because we're worried that it doesn't directly target the forms of interagency data sharing that put New Yorkers most at risk. So, Chair Williams raised earlier in the hearing the issue of data sharing with law enforcement, specifically with respect to the gang's database. We're worried that the current Data Protection Act allows for a fair amount of interagency sharing and doesn't specifically close the loopholes in the PPPL that allow for data sharing with law enforcement. So, while we find that-- the parts of the requirements of the Data Protection Act which require agencies to inform people what data is being collected and give people a slightly weaker data deletion requirement are useful. We're concerned that such goals might actually be better served by expansions of the PPPL that specifically close the loopholes around data sharing with law enforcement agencies. We applaud the role of the Data Protection Act in expanding data sharing restrictions to municipalities as well as state agencies, but we find that it might actually be less legislatively thorny to expand the PPPL directly instead of adding this separate Data Protection Act

to address those issues. Thank you for the opportunity to testify.

CHAIRPERSON GUTIÉRREZ: Thank you. And we have your testimony? Yeah, okay, thank you.

TALIA KAMRAN: Hi. Good afternoon. My name is Talia Kamran. I'm a staff attorney at the Seizure and Surveillance Defense Project at the Brooklyn Defender Services. Like both Chairs have opened the hearing with, New York City has entered a period in which the collection of data is built into nearly every interaction a person has with a city agency. And at the same time, digital police presence has expanded across agencies serving the poor, unhoused, and disabled New Yorkers. And now, individuals who already face higher risks of police harassment and violence are even more visible to law enforcement. This entanglement reinforces the school to prison pipeline, the criminalization of poverty and it turns services meant to help New Yorkers into additional surveillance touchpoints. And as public defenders we see how pervasive data collection and surveillance have deteriorated constitutional protections for the people we represent, and because such surveillance tech rarely enters the courtroom,

individuals subjected to these technologies have no opportunity to challenge these tools. The normalization of stripping poor and working class New Yorkers of their privacy and civil rights has to come to an end, and updating our data protection laws is a crucial first step. For these reasons, BDS strongly supports Intro 1335. This legislation recognizes that residents' digital identities are no different than physical identity and require the same level of protection. BDS also supports Resolution 783 in support of the New York State Data Protection Act. Statewide consistency will help ensure that New Yorker's sensitive information is safeguarded no matter which agency collects or stores it. But although Intro 1335 and Resolution 783 take important steps towards modernizing privacy protections, the city can't respect the fundamental right to privacy without also pulling back on discriminatory surveillance tools that undermine those protections outright. Along with data protection legislation, City Council must stop the inappropriate data collection. As an example, the NYPD gang database. We've known for years that the database overwhelmingly targets Black and Latino youth and

isn't a resource for violence prevention, and the database is vulnerable to abuse and information leaks as we've already seen ICE rely on false gang allegations to justify arrests and deportation. Even with legislation like the Data Protection Act which would limit data leakage, the mere existence of this repository creates an unjustifiable risk. The time has urgently come for City Council to vote and pass Intro 798 to abolish the gang database. And the concern over excessive data gathering extends beyond the NYPD. Systems like Securis [sic], the jail call recording software used in New York extract voice prints, a form of biometric data that would rightly fall under the expanded definition contemplated in 1335. But this information shouldn't simply be protected or regulated. It shouldn't be gathered at all. In order to protect New Yorkers' privacy, City Council must also pass the Echoes [sic] Bill and end surveillance of incarcerated people and their loved ones on calls. In closing, Intro 1335 and 783 are essential steps towards modern privacy protections, but we have to pair them with limits on harmful surveillance tools. Thank you for the opportunity to testify.

CHAIRPERSON GUTIÉRREZ: Thank you. Okay. Thank you. No questions. Next panel, Susan Peters, Richie Lipkowitz-- my apologies if I'm mispronouncing that-- and Alex Spryropoulos. Alex, also my apologies if I'm mispronouncing that. My bad.

RICHIE LIPKOWITZ: I've been designated to start off. So, let me say thank you to Jennifer and Nantasha for revealing-- I wouldn't hold your breath for letter of reply on December 18th. But it reveals what's going on with AI. AI is here. I've been sending to your office-- some weeks ago-- well, maybe some months ago already, there weren't that many AI articles in the New York Times. Now, it's twice a day. And we have every reason for privacy to be scared. I'm hoping the new administration will be more amenable to dealing with issues that will face us because AI is already here whether we like it or not. Thank you.

CHAIRPERSON GUTIÉRREZ: Thank you. Thank you, Richie. Alex?

ALEX SPYROPOULOS: Good afternoon, Madam Chairs. Thank you for the opportunity to testify today on privacy protection in the digital age. My name is Alex Spyropoulos. I'm here on behalf of Tech

NYC which represents more than 550 technology companies across New York's tech ecosystem. Our members share a common belief, privacy and innovation and not at odds. In fact, strong and thoughtful privacy protections are essential to building the public trust that fuels innovation. In the absence of a federal privacy standard, more than 20 states now have enacted comprehensive data privacy laws. Tech NYC believes that New York should do the same, adopting a clear, statewide framework that protects consumers, provides clarity for businesses, and aligns with the model already covering over 100 million Americans. Interoperability isn't just about efficiency, it's about fairness. New Yorkers deserve the same rights and protections whether they're interacting with a company based here, in Connecticut, or in California. A consistent approach makes compliance manageable for businesses of all sizes while giving consumers confidence and control over their data. Finally, as we consider how to govern emerging technologies like artificial intelligence, it's important to remember that responsible AI governance starts with data privacy. Without clear guardrails around how data is

collected, used and protected, we can't ensure that innovation happens responsibly. New York has always been a leader in technology and policy. This is our chance to lead again by creating a privacy framework that empowers people, supports small businesses and strengthens trust in the digital economy. Thank you for the opportunity to testify today.

SUSAN PETERS: Hi. I'm Sue Peters. I'm a resident of Manhattan Community Board Seven and also a consulting party for the National Historic Preservation Act for the placement of cell towers in Manhattan Community Board Seven. I wish to speak on the centralization of the Federal Government in alliance with the FCC and private telecoms which are currently attacking our local controls over cell towers and antennas placements over the entire USA, but of course I'm concerned about where I live. We're losing our privacy with the introduction of a wireless control grid. This is constitutional. December 1st this year, the FCC published rule 25-67 and proposed rule changes to destroy all local control over cell tower deployment and changes to them. In other words, no public hearing, no environmental review, no advance notice to neighbors,

no radio frequency compliance certification to be done on the antennas, no ability to deny cell towers by local government. Under cover of the COVID pandemic in 2020, this process began when telecom trucks rolled out to install broadband from power pole to power pole. Left was to attach the antennas which is now they're attack. Reminder, in 2021 the DC Circuit Court said the FCC must respond to 20,000 pages of documentation of physical harm by the FCC's 1996 RF threshold which the FCC has ignored 'til today and not responded to the court. November 2025, the federal House Subcommittee on Energy and Commerce introduced 28 bills including HR2289. December 3rd, one week later, the federal Committee on Energy and Commerce consolidated these 28 bills to 15 and along with HR2289 sent them to the full House. HR2289 especially is a coup against local government and environmental protection. One Congressman during the committee hearing said let's get rid of these pesky protections. So, forget about protecting our churches, our schools, our parks, our sidewalks, our streets, no protection through local control. The FCC and private telecoms are used in Congress against local control. This is being done during the holidays

when people are extra busy. Please investigate and fight this. Thank you.

CHAIRPERSON GUTIÉRREZ: Thank you so much. Thank you for your testimony. The next panel is Beverly Blondmonville and Michele Blondmonville.

MICHELE BLONDMONVILLE: Hello. My name is Michele Ann Blondmonville, and I'm adding onto what the last testifier said. Thank you for your servitude in these difficult times. I'm speaking on behalf of everyday people who have Havana Syndrome or anonymous health incident victims, some knowingly and some others unknowingly. This glaring awareness of the benefits afforded our diplomat counterparts helping American victims affected by neurological attacks, Havana Act of 2021, public law 117-46. We certainly [inaudible] that one day we'll be free from torture, pain, and disability, and the weaponization of technology. Havana Syndrome includes remote access to the biology of a human being. Yes, it's-- they use radio frequencies in order to attach themselves to our biometric. Everyday people Havana Syndrome victims is comprised of diagnosed Havana Syndrome public citizens who have been unlawfully experimented on or who endured 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, nonconsensual human experimentation socially and technologically such as B2K, blue [sic] eye technology, and AI. They are put on [inaudible] knowingly that are distributed to various agencies for this experimentation for vindictive reasons, technological research, and political harassment. No one should have their brain interfaced to a computer or AI program. We're assaulted 24 hours a day randomly for compliance and are remotely neuro [sic] monitored. We would like New York to adopt laws that protect our normal data like California law SB1223 and Colorado health bill 24-1058 protecting brain [inaudible] collected by devices. And also, recently Texas House Bill 2715-- also, repeal the Patriot Act allowing various agencies to experiment on innocent public citizens, and for this reason I am in favor of all laws that protect our privacy and neuro data, including Intro 1335, Intro 1340, Intro 1367, Resolution 0783, and Resolution 1062. Thank you.

BEVERLY BLONDMONVILLE: Good evening. My name is Beverly Blondmonville. I'm a resident of Queens, Council District 27. I have worked at Chase Manhattan Bank for most of my life, my 20s onto retirement as a technology analyst. I was involved in the Y2K ATMs, making sure the technology was in compliance for the entry into the 21st century. Now, I am in my retirement, and I find myself being experimented on with remote technologies. As the gentleman said, AI is here, but there are no rules. There aren't sufficient rules, and they're free to do whatever they want, whatever they want. This journey has been excruciating and painful. I am tortured 24 hours, seven days a week, at the mercy of whoever has access to my biometrics, I am one of quite a few people. I am asking for advocacy and support to protect my rights. I did not consent to any of this. And for this reason, I am in favor of all laws that protect our privacy and neuro data, including Intro 1335-2025, by Jennifer Gutiérrez, Intro 1340-2025 by Farah N. Louis, Intro 1367-2025 by Yusef Salaam, Resolution 0783 by Ms. Nantasha Williams, Resolution 1062 by Kamillah Morris [sic]. Thank you for your consideration.

CHAIRPERSON GUTIÉRREZ: Thank you both. Thank you so much. We will now turn to our witnesses joining us via Zoom. First up is Cynthia Conti-Cook, followed by Christopher Leon Johnson.

CYNTHIA CONTI-COOK: Hi, good afternoon. Thank you for the opportunity to testify. Thank you to Chair Gutiérrez and Dr. Williams and to the members of the Technology and Civil and Human Rights Committee for the opportunity to testify. I'm testifying on behalf of the Collaborative Research Center for Resilience in support of Intro 1335 and also with support of Resolution 783, although I share the concerns mentioned previously about the gaps regarding interagency data sharing. We testify to raise awareness about how recent developments in data sharing, privacy protocols, and pending state legislation under the One City Act pushed by the outgoing administration over the past three years have undermined New Yorkers' expectations of privacy in relation to their personal identifying information when it collected for the purposes of accessing city services. It is important to remember what was happening when the initial privacy protections were enacted. In 2017, as the first Trump administration

initially threatened our immigrant communities, New Yorkers broadly supported City Council bills that articulated an expectation of privacy on behalf of all New Yorkers in relation to the identifying information they share in order to access services alongside a slate of other laws intended to protect New Yorkers from seizure and separation from their communities. Local Laws 245 and 247 were clearly intended to make all New Yorkers safer by protecting personal identifying information from being seized for profit or virtual patrolling. New Yorkers recognized that protecting broad access to safety net services for all who need them keeps us all safe. Vigilantly protecting these laws are even more important now. Over the past three years, the outgoing administration made several attempts to corrode these protections, for example, through MyCity data sharing agreement in March 2023 which we've previously testified about and raised in our March 2024 report, MyCity Inc, and most recently through expansions to citywide privacy protocol changes made in 2025, that as Chief Privacy Officer Fitzpatrick explained directs Agency Privacy Officers to defer without question to NYPD demands for

disclosures without substantiation. This latter maneuver broadens the already too large loophole that the NYPD and other law enforcement agencies and many others enjoy and should be revisited, especially given the example named by Dr. Williams and recent reporting about NYPD data sharing with the federal government. While Intro 1335 hopefully expands the definition of identifying information, it's time to apply these expectations of privacy to police disclosures and require reporting by police about how the data they seize through technology data sharing agreements and personnel stationed to agencies throughout the city impacts New Yorkers. I also wanted to raise attention about the One City Act legislation that was pushed by the outgoing administration in Albany in 2023 and 2024 which would specifically undermine the intention of the 2017--

SERGEANT AT ARMS: [interposing] Your time has expired.

CHAIRPERSON GUTIÉRREZ: Can I ask a question, one question, Cynthia? Thank you for your testimony. How concerned are you about AI's ability to combine different data points to identify a person even when individual pieces of data seem anonymous?

CYNTHIA CONTI-COOK: Absolutely very concerned. The capacity of AI technologies to triangulate different sources of information and use that to identify someone has already been very well documented by computing scholarship.

CHAIRPERSON GUTIÉRREZ: And what is-- I mean, you reference this a little bit in your testimony, but what does the One City Act mean for New Yorkers and our data?

CYNTHIA CONTI-COOK: While, the One City Act has a very good intention which is to make benefits for New Yorkers more accessible, it creates a very large loophole, and the outgoing administration was specifically pushing the purposes of the One City Act as being-- helping NYPD gain access to, for example, mental health and other health information when removing people from subways, removing people from parks and sidewalks, and to facilitate the harvest of personal data through the MyCity portal. Those were the two use cases that the One City justification specifically described, and the One City Act unhelpfully identifies as the Human Services Agency, any agency that does crime prevention, and so while it is forward-- it is

apparently for the purposes of benefits access, it does allow a great deal more law enforcement access into city service agency data.

CHAIRPERSON GUTIÉRREZ: Thank you. Thank you, Cynthia. And then our last Zoom panelist is Christopher Leon Johnson.

CHRISTOPHER LEON JOHNSON: Yeah, hello. My name is Christoper Leon Johnson. Thank you for having this hearing, Chair. I support both Chair Williams and Gutiérrez. I support Nantasha Williams bill when it comes to making aware that the state agencies must not be sharing [inaudible] make sure that they don't-- with [inaudible] make sure that they don't share the information with third-party agencies, but I want to make this clear that, I believe that the City Council-- not only City Council-- I believe that the state need to make it where that they need to stop sharing people-- our information with the nonprofit sector, because of course, like, we have a big problem with third-- like, corporations taking our data, but the big-- one of the bigger issue when you start, like I am, is that the nonprofit industrial complex, especially the homeless industrial complex, what they do is they

get-- they bring some of their lobbyist friends and consulting friends, and they weaponize the influence. They weaponize-- they do every dirty trick they can do to try to work with some of these people that work in City Council to [inaudible] rank and file staff members to start within all the office. Even the members that work directly with the Speaker, and they leak out the information. They give this information to the nonprofit people that run these nonprofits in exchange for money. Not to say that members of City Council is doing it themselves, but there's a way to make money through selling data, illegally selling data. What needs to start happening more in the City Council is to make it where that it's-- make it really illegal to start giving data to the nonprofits and aware that-- then you start training employees to where to be careful of the people that they mingle with at these holiday functions and these galas and these community events, because that's how they creep in and now they got you. So I think more-- what need to start happening more is that the City Council have to start being the first put forward and make it where that they need to have more training with the employees. Not only the Sergeant at Arms, it could

be the people that work the tech, it could be people that do the media, or everybody with the City Council to where that-- the watchout who's their friend who's trying to use them, because this is a big serious topic. It's really serious. We have-- you got people who are bad faith actors who act like they're the friends, and they come out and want to steal data. So, I think that'd even be the conversation more going forward. But I support all the bills. I get it 100 percent. We have to protect our identities from deepfake and the City Council has to make it where that AI is not influencing the City Council. And I'm calling on the City Council to denounce Alex Bores, the State Assembly Member Alex Bores because he's the main guy in city government that is pushing AI in government. And I think the City Council, it started with the members that live in the 12 council-- the 12 congressional district like Council Member Eric Bottcher and Julie Menin and Gale Brewer and Padrino [sic], and all these elected [inaudible] powers should make a public condemnation of Alex Bores, because he's the biggest public trader--

SERGEANT AT ARMS: [interposing] Your time is expired.

CHRISTOPHER LEON JOHNSON: deep fakes and AI in government, so--

CHAIRPERSON GUTIÉRREZ: [interposing] Thank you.

CHRISTOPHER LEON JOHNSON: all I got to say. Thank you so much. Enjoy your day.

CHAIRPERSON GUTIÉRREZ: Thank you. Thank you, Christopher. Our final panelist is Odette Wilkens. One second. We're unmuting you. One second, Odette, we're just-- we're unmuting. You can try now. It still--

ODETTE WILKENS: Hello?

CHAIRPERSON GUTIÉRREZ: Yes, now we can hear you. We can hear you now. You can start. Odette, do you want to start? We can hear you. Oh, she can't hear us? Can you hear us now, Odette? Yes? Go for it. And can you--

ODETTE WILKENS: [interposing] Okay, I can hear you now. I couldn't-- I couldn't hear anything before.

CHAIRPERSON GUTIÉRREZ: No, no, that was our bad. That was our bad. Your time starts now. Thank you.

ODETTE WILKENS: Okay, fantastic. I hope my computer doesn't run out of batteries. Okay, I'm Odette Wilkens and I'm President and General Counsel of the Wired Broadband Inc, and we're a nonprofit advocating for safe communications infrastructure, and I'm also Executive Director of the New York City Alliance for Safe technology. We are talking about privacy and security, and one of the things that we haven't been talking about is how the communications infrastructure that we're deploying in New York City including-- especially 5G-- is housing challenges to privacy and security. I want to call your attention to a letter that was sent to the National Telecommunications and Information Administration 2020 by New York City's Chief Technology Officer and Chief Information Security Officer spotlighting 5G's security vulnerabilities. 5G, because of its architecture, is inherently insecure. The former FCC Chair, Tom Wheeler, specified that-- has called it the 5G Cyber Paradox, because 5G is a software-based system. It is not a hardware-based system. So if

there is a security breach, it's not each to quarantine the breach. 4G and 3G are hardware-based systems so it's easy to quarantine a security breach. You can't really do that with 5G. Again, access to one 5G note, you can access to the entire network, especially with millions of 5G nodes out there, it increases the service areas for hackers. So that's something that we need to look at. Alnd also we need look very closely at the agreements that city bridge and the city have had, and the city has had with other [inaudible] franchisees. Because one of the things that it wanted to bring to your attention is that the privacy policy in this city's franchise agreement, the City Bridge, for instance, states that the City Bridge does not support a do not track function. Therefore, users and children's online activities can be tracked. So, if city Bridge also states that oh, they do not collect information about your precise location, they can determine your general location when you're using their services. Now, OTI has stated that personal information would not be exploited by City Bridge, but the policy privacy states that third-party providers would be managing email addresses without a stated obligation

in the contract that those providers would maintain confidentiality and would also not exploit personal information. So, we're talking about City Bridge. City Bridge. City Bridge won't display it, but how about their third-party providers? So, and of course, the bridge sates that it cannot guarantee against access to personal information by unauthorized third-parties. So, this is something that we really need to look at in terms of a 5G deployment, and also the New York Civil Liberties Union has warned that LINK NYC network has significant privacy vulnerabilities with this collection of personal information including email addresses, browsing data, and camera surveillance. And changes were reported to have been made to alleviate those concerns, but serious doubt still remain at the New York City Civil Liberties Union. So we really need to look at that. Then also I don't know if you about the U.S. Senate has introduced the Mind Act in order to prevent the use of people's brain information, neuro data--

CHAIRPERSON GUTIÉRREZ: [interposing] Odette, can you please wrap up?

ODETTE WILKENS: Okay, yeah. So that's something to also keep in mind that we don't want neuro data to be exploited, and that's in the Mind Act of 2025 that was introduced in the U.S. Senate. Thank you very much.

CHAIRPERSON GUTIÉRREZ: Thank you for testifying and if you could also just make sure that we get the copy of a letter that you said at the top of your remarks? Thank you. Okay, if we-- I think that was the last panel. If we have inadvertently missed anyone who has registered to testify today and has yet to have been called, please use the Zoom hand function and you'll be called in the order that your hand has been raised. Nobody? Thank you everyone for your testimonies. Thank you so much to my bomb Co-Chair. This is the last hearing, hearing of the year. The hearing is adjourned. Thank you to both teams.

[gavel]

C E R T I F I C A T E

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

Date December 22, 2025