NYC Cyber Command

NYC Mayor's Office of the Chief Technology Officer

June 25, 2020

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

RE: The National Strategy to Secure 5G Implementation Plan
[Docket No. 200521–0144; RIN 0660–XC047]

The City of New York (City) appreciates the opportunity to comment on the development of an Implementation Plan for the National Strategy to Secure 5G. The following comments are based on New York City's own implementation plan (the NYC Internet Master Plan), released in January 2020, and the efforts of NYC Cyber Command (NYC3) to ensure strong cybersecurity practices for current and new technologies used by and within the city.

Affordable, reliable, and equitably distributed high-speed internet access is critical to the economic and personal well-being of the city's nearly 8.4 million residents. Currently, broadband services available from private companies continue to leave behind too many New Yorkers. While a majority of New Yorkers do have access to broadband, more than 1.5 million residents still have neither a connection at home nor on a mobile device.

Our city is committed to fighting income inequality and ensuring all New Yorkers have opportunities to succeed. That means every New Yorker should have affordable and reliable access to high-speed broadband so that they have access to quality educational opportunities, health care, and essential services. As the recent COVID-19 pandemic has laid bare, access to reliable broadband is now a prerequisite, similar to a public utility, to ensure personal safety, education, and opportunities for economic growth for New Yorkers.

As outlined in the NYC Internet Master Plan, 5G technology is uniquely well-suited to a dense urban environment such as New York and we recognize the importance of ensuring that 5G is deployed in a manner that contributes to closing the digital divide, not widening it.

While this new technology brings the potential for great opportunity, its deployment brings new risks and national security concerns. As a center of commerce with a gross domestic product that rivals many nations, New York City is a target for economic espionage by foreign governments. Our city is home to some of the largest corporations in the United States, as well as an innovative and thriving startup culture. Emerging technologies built in New York City drive over $70 billion in startup valuation and exits each year. 5G represents a new threat vector for nation-states and other foreign actors intent on stealing intellectual capital from our residents.

Beyond economic interests, there are political and cultural reasons our city is a high-profile target for adversaries that seek to undermine the integrity of our infrastructure for other nefarious purposes.

Technology components critical to the rollout of 5G in the U.S. will almost certainly require significant (if not critical) reliance on foreign technology firms, manufacturers, and their supply chain ecosystems—particularly China, who has historically sought to "access information about U.S. firms' proprietary operations and project-financing information, as well as steal IP and technology" through cyber espionage, according to the U.S.-China Economic and Security Review Commission. This creates a significant supply chain risk.

New York City is highly concerned about the threats created by a lack of coherent national vision and strategy for securing our nation's telecommunications infrastructure. This lack of federal leadership domestically and in coordination with allies internationally makes our city vulnerable to foreign adversaries who may seek to undermine us.

For these reasons, we urge you to consider: 1) funding for state and local testbeds, development, security controls and other factors necessary in furtherance of a secure 5G deployment; 2) national authorities and standards for rigorous, ongoing testing to secure 5G technology components, as well as the devices that utilize 5G networks; 3) federal regulatory structures that provide safeguards against the risk of the increased attack surface that is likely to arise along with mature 5G network development; and, 4) engagement with key international allies on this critical national security issue.

Line of Effort 1: Facilitating Domestic Rollout

To facilitate the domestic rollout of 5G technologies and the development of a robust domestic 5G commercial ecosystem (e.g., equipment manufacturers, chip manufacturers, software developers, cloud providers, system integrators, network providers), the City urges the federal government to consider and address security-related supply chain concerns. The City is troubled by disruptions to the 5G ecosystem that are likely to increase the cost and reduce the efficiency of any 5G technology deployment, but may prove necessary to curtail systemic security concerns. Private and public investment will be vital to ensuring affordable, reliable high-speed access is available across the five boroughs of our city, ensuring all New Yorkers have access to the economic, social, and civic power of the internet.

The City recognizes the critical role that advanced technologies play in national security. Investment in the research, development, testing, and evaluation of new technologies and architectures can launch mutually-beneficial public and private partnerships through federally-funded research projects. In the near term, New York recommends federal funding for local municipal investment in secure 5G network infrastructure in an effort to promote specific security requirements around 5G network equipment and infrastructure. We will discuss more about mitigating the significant equipment-related security concerns in our response to other Lines of Effort.

The City also invites meaningful research partnerships given that we maintain one of the most appropriate environments for 5G technologies. For instance, with funding from the National Science Foundation Platforms for Advanced Wireless Research and through partnerships with academic researchers and industry stakeholders, a wireless testbed in Upper Manhattan, named COSMOS, serves as a real-world research hub for new wireless technologies and applications in one of the most populated urban environments in the world. These kinds of testbeds are necessary to ensure the appropriate scientific and technical knowledge is developed to advance new and more secure products to the market that work in many environments, including environments like New York City that require consideration of security factors unique to densely populated and urban areas.

In addition, to increase domestic 5G research, development, and testing, New York City would invite an opportunity to serve as the site for an "X-Prize" or DARPA grand challenge-style scientific innovation investment opportunity that looks to foster a secure, domestically produced 5G commercial ecosystem. This would mirror other investment approaches that have brought the United States to the forefront of ingenuity and production in certain industries—perhaps most notably in the areas of autonomous vehicles and private sector spaceflight—with investments from public and private sector entities. New York City has served as host to federal pilots and partnerships to promote telecommunications technology, including our joint effort to improve the safety of travelers and pedestrians through the deployment of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) connected vehicle technologies. We look forward to welcoming such innovation again.

Line of Effort Two: Assess Risks to and Identify Core Security Principles of 5G Infrastructure

5G's potential for higher speeds and other advantages also brings system complexities that may not have existed in previous generations of broadband technologies. The dynamics of 5G make this technology much less like a traditional

telecommunications platform and more like the multi-layered open environment we find on the internet. Such complex systems present more opportunities for security and privacy breaches. By moving away from firmware-based technology of 4G telecommunication components to software-based 5G telecommunication components that will need to be updated, the opportunity for manipulation exists within the supply chain. Furthermore, movement away from centralized network systems to decentralized network systems increases the attack surface of a network. That increased attack surface is amplified by the anticipated introduction of the increasing number and variety of connected devices (IoT) and big data industries.

Core security principles for 5G should be built upon existing foundational security principles and programs. For example, federal standards for supply chain risk analysis have been built by the National Institute for Standards and Technology (NIST), which should be highly leveraged on the federal level and made mandatory for access to grants for deploying new telecommunications platforms, such as the ones we discussed in Line of Effort One. It should also be foundational to federal investment in the technology more generally.

New York City Cyber Command has built an Internet of Things (IoT) Lab to rigorously test publicly-owned connected devices prior to citywide deployment. Our work confirms what is well known and evident: the risk inherent in these lightweight technologies. IoT risk profiles change with their environment and specific use case, and security has generally not been the primary focus of manufacturers of these technologies. We have identified dozens of critical and high risk vulnerabilities within proposed devices. Many have already been deployed elsewhere in the country and world prior to New York City's review. New York City Cyber Command has also identified "zero-day" (previously unknown) exploits that now have published common vulnerabilities and exposures (CVEs) associated with them. These vulnerabilities have been resolved by the vendors prior to deployment in our municipality, and ultimately benefits the public and private sector by improving security.

The problem of IoT vulnerabilities will only become exacerbated by the increased speeds of 5G and other future wireless broadband technologies.

Similarly, several significant vulnerabilities have been discovered by security researchers during initial 5G rollouts in test markets. As with any new technology, it is likely that additional, potentially critical, zero-day vulnerabilities exist within 5G technology components.

We recommend the federal government provide grants to localities and states for rigorous security testing of critical devices being considered for adoption by the public sector and critical infrastructure partners. This becomes vital with the anticipated expansion of IoT device use commensurate with the increased load and speed capabilities of 5G networks.

Additionally, New York City recommends federal testing and security requirements for consumer grade IoT devices. IoT protection is historically poor and malware distribution is easily scalable, which suggests that the creation of IoT botnets ("robot networks") for malicious purposes, including large-scale distributed denial of service (DDoS) attacks, is likely to increase as well. This poses a significant threat to vital digital infrastructure and resident services at all levels of government, as well as private sector enterprise.

New York City has dedicated itself to supporting our residents' secure connectivity as the cyber threat environment has continues to escalate. New York City Cyber Command, created in 2017, is charged with securing our public infrastructure and supporting the digital security of New Yorkers. New York City Cyber Command has built security-driven solutions into public Wi-Fi connectivity points and offers our residents mobile threat protection through NYC Secure, the first-of-its-kind free mobile security application from a public entity. In addition, the City has proposed baseline and additional security standards for a higher-level of service for users of public Wi-Fi on city streets in its Truth in Broadband: Public Wi-Fi in New York City report. Such consumer-facing initiatives at the local level should be supported through federal funding to

identify and raise best practices for raising cybersecurity support for the general public to meet the accelerating threat environment.

Finally, the federal government should require regular independent testing and certification of 5G telecommunication components. This testing will need to occur on a regular basis to ensure changing software does not create new vulnerabilities, and build processes for resolution when security concerns are identified.

Line of Effort Three: Address Risks to U.S. Economic and National Security during Development and Deployment of 5G Infrastructure Worldwide.

The passage of the Secure 5G and Beyond Act of 2020 by Congress is just one step in addressing the risks to economic and national security in the development and deployment of 5G infrastructure. We believe a lack of national strategy leads to inconsistent international engagement around our telecommunications infrastructure. While there have been specific instances where the federal government has pushed allies away from equipment associated with foreign adversaries, such activity is not a substitute for a proactive and comprehensive approach to a complex technology market. This dynamic creates a significant security risk to our city's critical infrastructure, as well as to the privacy and economic security of our residents.

In essence, New York City is executing on our security strategy in absence of the perspective of a comprehensive federal framework. While there is no scenario where governments lead the development and deployment of 5G and future telecommunications technologies, the public sector must play a critical role in its development and deployment. From international coordination among allies, to national leadership in the executive branch, to support for state and local deployment strategies, the required federal orchestration and influence has been largely absent.

The City shares the concerns outlined in the U.S. Senate Committee on Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations staff report released earlier this month that pointed to a lack of authority and process at the federal level as key factors which undermine a cohesive telecommunications review of foreign actors, endangering our national security.

New York City urges the federal government to coordinate investment from federal and private sources into research and development of domestic telecommunications technologies at public and private institutions, while creating a coordinated effort among allied countries to do the same. Beyond attempting to gain primacy in domestic 5G manufacturing, efforts should be focused on accelerating the timeline and early production of other domestically nurtured next-generation telecommunication "6G" technologies in concert with key allied nations. The City also encourages the federal government to promote 5G vendor diversity and foster market competition, so long as these actions do not negatively impact or otherwise disrupt paramount security considerations and initiatives.

Line of Effort Four: Promote Responsible Global Development and Deployment of 5G.

An effective policy and regulatory framework which outlines equitable standards, incentives, and sufficient enforcement mechanisms is essential for promoting and facilitating global development and deployment of 5G. However, this framework should prioritize and support—not displace or disrupt—5G deployment and implementation initiatives at the state and local levels that provide for necessary security protections and public services that benefit city residents and businesses.

Continued disagreements and disarray among federal actors and telecommunications sector stakeholders on issues ranging from infrastructure security and supporting state and local broadband deployment efforts to confronting foreign

disinformation campaigns focused on undermining our democracy is ultimately allowing foreign governments to fill the void and set standards for security and privacy in the global tech industry. Widening the gap further are federal actions that favor large telecommunications companies at the expense of consumers and local governments, including the elimination of privacy protections, affordability programs and net neutrality requirements. We can only succeed through communicating American values of inclusiveness and digital rights nationally, promoting those values internationally through strong alliances with international partners, such as New York City's participation in Cities for Digital Rights, and ultimately constructing a common vision built upon mutual security.

To promote responsible global development and deployment of 5G, the federal government must stand up for our values by: 1) not impeding the abilities of states and localities to take necessary and appropriate actions, such as those discussed in the New York City Internet Master Plan, that promote and facilitate broadband services and enable affordable, equitable, reliable, secure high-speed broadband deployments within their communities; 2) providing funding, necessary authorization, and guidance to federal agencies tasked with monitoring foreign manufacturers and telecommunications carriers; and, 3) focusing on engaging our international allies to build standards that provide mutual security assurances.

Thank you for your dedication to this issue. We stand ready to work with our federal partners to secure our nation's vital telecommunications infrastructure and ensure the availability of secure high-speed, reliable, quality broadband service for all New Yorkers.

Sincerely,

Geoff Brown

Chief Information Security Officer
City of New York

John Paul Farmer

Chief Technology Officer
City of New York

Office of Technology & Innovation

OFFICE OF TECHNOLOGY AND INNOVATION TESTIMONY BEFORE THE NEW YORK CITY COUNCIL COMMITTEES ON TECHNOLOGY AND CIVIL AND HUMAN RIGHTS

Oversight - Privacy Protection in the Digital Age: Balancing Technological Advancements with Privacy Protections.

Int 1335-2025: 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

Int 1340-2025: 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

Int 1367-2025: A Local Law to amend the administrative code of the city of New York, in relation to a top-level domain name requirement for websites maintained by city agencies

December 8, 2025

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 (OTI) 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 toolkit 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, or 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 are 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 include:

- 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 Information 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 (IAPP), 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 (TEC) 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 1335-2025 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 other 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 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 am happy to discuss this further with the Council.

Introduction 1340-2025 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 (AI) 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 1367-2025** 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.

###

JUMAANE D. WILLIAMS

TESTIMONY OF PUBLIC ADVOCATE JUMAANE D. WILLIAMS
TO THE NEW YORK CITY COUNCIL COMMITTEES ON TECHNOLOGY AND CIVIL AND HUMAN RIGHTS
DECEMBER 8, 2025

Good morning,

My name is Jumaane D. Williams, the Public Advocate for the City of New York. I want to thank Chairs Gutierrez and Williams as well as committee members for holding this important hearing and allowing me the opportunity to testify.

There exists a delicate balance between our civil liberties and our public safety or national security. One does not have a First Amendment right to scream "Fire" in a crowded room. However, this balancing act is critical and indispensable when technological advances are taken into consideration since public safety and national security can be compromised globally in a nanosecond. New Yorkers are no strangers to surveillance overreaches made in the name of public safety, the lasting trauma that comes from having our civil liberties — the right to privacy and often our right to equal protection under the law — denied. In the wake of 9/11, we saw how our Muslim neighbors were profiled and surveilled, sowing fear and distrust amongst our communities. Individuals impacted by stop-and-frisk policies have continuously had their past records used to increase charges for unrelated crimes even decades later, despite two New York State laws requiring those records to be sealed or destroyed.[1] These same records have contributed to NYPD's facial recognition database.

With the advent of new technologies, specifically the proliferation of facial recognition, this administration has created an increasingly expansive and pervasive surveillance network. Even on his way out, Mayor Adams has facilitated the expansion of this network, ensuring that surveillance continues in his absence. A mere month after NY Focus reported NYPD utilized the Big Apple Connect program as a backdoor for undisclosed live video surveillance at New York

[1] Galvañ, Ana. "Your Arrest Was Dismissed. But It's Still In A Police Database". *The Marshall Project.* July 18, 2019. www.themarshallproject.org/2019/07/18/your-arrest-was-dismissed-but-it-s-still-in-a-police-database

City Housing Authority (NYCHA) developments and, more damningly, a day before a City Council oversight hearing on the matter, Mayor Adams extended Big Apple Connect contracts for an additional three-year period.[2] Under Big Apple Connect, the live video feeds from these public housing cameras link to a larger network known as the Domain Awareness System, used "to track crime and help identify suspects by synthesizing vast amounts of data from video, license plate readers, audio gunshot detectors, 911 call logs, criminal histories, summonses, arrests, warrants and more".[3] In a world where privacy grows increasingly scarce, New York City should not facilitate this type of digital surveillance. As the data broker economy continues to grow, there must be measures in place to protect New Yorkers' constitutional right to privacy. Furthermore, the enforcement of the Public Oversight of Surveillance Technology (POST) Act is critical for ongoing transparency and accountability.

In the larger national context, Immigration and Customs Enforcement (ICE) has been funded at the expense of nearly every part of our social safety net, acquiring powerful tools to surveil and identify individuals and communities, and working with local law enforcement to carry out raids. A report by the Department of Investigation released just last week, found at least one instance where an NYPD officer violated the city's sanctuary laws to coordinate with federal officials, as well as existing "gaps in the agency's policies and practices that raise the risk of improper information sharing or assistance to federal authorities for purposes of civil immigration enforcement".[4] We cannot allow this to become the new norm.

I look forward to working with the incoming administration to curtail these abuses, demystify opaque surveillance tactics and affirm New Yorkers' rights to privacy – digital or otherwise. Thank you.

---

[2] Groz, Zachary. "Adams Locks In Big Apple Connect Through 2028, One Day Before Oversight Hearing." *Focus.* September 29, 2025. https://nysfocus.com/2025/09/29/adams-big-apple-connect-renewal

[3] Cramer, Maria. "Mamdani, a Sharp Critic of Police Surveillance, Will Soon Oversee It". *The New Times.* November 30, 2025. www.nytimes.com/2025/11/30/nyregion/mamdani-tisch-nypd-surveillance.html

[4] "DOI Investigation into the NYPD's Compliance with Local Laws Restricting City Assistance with Immigration Enforcement." *New York City Department of Investigation.* December 3, 2025. https://www.nyc.gov/assets/doi/reports/pdf/2025/49NYPD.SancLawsRelease.Rpt.12.03.2025.pdf

Testimony on Privacy Protections in the Digital Age

Tech:NYC Written Testimony— Last Updated: 12.8.25

Thank you for the opportunity to submit testimony as the Committee on Technology explores the topic of Privacy Protection in the Digital Age: Balancing Technological Advancements with Privacy Protections. Tech:NYC, which represents more than 550 technology companies operating and growing across New York, from early-stage startups to some of the world's largest and most established technology firms, has been working on the topic of data privacy for the last several years at the State level. We appreciate the opportunity to share the perspective of New York's tech community. The technology sector is broad and diverse, comprising not only global leaders but also numerous small businesses, entrepreneurs, and mission-driven organizations that rely on responsible data use to power their products and services.

Across this ecosystem, there is a shared recognition that privacy and innovation are not mutually exclusive. Strong, thoughtful privacy protections help build public trust, which is essential for continued technological progress.

The Need for a Comprehensive State Data Privacy Framework

In the absence of a federal privacy standard, states across the country have stepped forward to establish their own data privacy frameworks. Over twenty states have already enacted comprehensive laws that define clear consumer rights, business responsibilities, and enforcement mechanisms.

Tech:NYC has been actively engaged in efforts over the last few years to work toward New York State adopting a comprehensive, sector-agnostic, and interoperable data privacy law. A state framework that aligns with emerging national models would ensure consistent protections for consumers while reducing compliance burdens for businesses that operate across multiple jurisdictions.

Interoperability and Consumer Trust

Interoperability is not just a matter of efficiency. It is also a matter of fairness and clarity for consumers. New Yorkers should enjoy the same privacy protections whether they are interacting with a company based in New York, Connecticut, or California.

Aligning with nationally recognized frameworks will give consumers predictable rights, such as access, correction, deletion, and transparency. It will also give businesses the clarity they need to comply responsibly.

Privacy as a Foundation for Responsible Innovation

As policymakers at every level grapple with emerging technologies such as artificial intelligence, it is important to recognize that effective AI governance begins with a strong foundation in data privacy. AI systems are built on data, and without a clear legal framework governing data collection, use, and protection, New York risks lagging behind other states in both innovation and consumer trust.

By bringing New York up to the standards established in more than twenty other states in the data privacy realm, the state can ensure that future innovations, including AI and connected devices, are developed and deployed responsibly.

Conclusion

New York has long been a global leader in innovation, creativity, and policy. The opportunity before us is to extend that leadership into the realm of data privacy by crafting a framework that empowers individuals, provides clarity for businesses, and supports innovation across the state.

Tech:NYC and our member companies stand ready to work with the Council, the State Legislature, and other stakeholders to advance thoughtful privacy protections that reflect New York's values and leadership in the digital economy.

Sincerely,
Alex Spyorpoulos
Director of Government Affairs
Tech:NYC

Brooklyn Defenders

Brooklyn Defender Services
177 Livingston St, 7th Fl
Brooklyn, NY 11201

Tel (718) 254-0700
Fax (347) 457-5194
info@bds.org

TESTIMONY OF:

Talia Kamran, Staff Attorney

BROOKLYN DEFENDER SERVICES

Presented before

New York City Council Committees on Technology and Civil & Human Rights

Oversight Hearing on Privacy Protection in the Digital Age

December 8, 2025

My name is Talia Kamran and I am a Staff Attorney in the Seizure and Surveillance Defense Project at Brooklyn Defender Services. Brooklyn Defender Services (BDS) is a public defense office whose mission is to provide outstanding representation and advocacy free of cost to people facing loss of freedom, family separation and other serious legal harms by the government. We are grateful to the Committees Technology and Civil and Human Rights, and Chairs Gutiérrez and Williams for inviting us to testify about privacy protection in a time of rapid digital information collection.

For nearly 30 years, BDS has worked, in and out of court, to protect and uphold the rights of individuals and to change laws and systems that perpetuate injustice and inequality. After 29 years of serving Brooklyn, we recently expanded our criminal defense services to Queens. We represent close to 40,000 people each year who are accused of a crime, facing the removal of their children, or deportation. Our staff consists of attorneys, social workers, investigators, paralegals and administrative staff who are experts in their individual fields. BDS also provides a wide range of additional services for our clients, including civil legal advocacy, assistance with educational needs of our clients or their children, housing and benefits advocacy, as well as immigration advice and representation.

Background

New York City has entered a period in which the collection, storage, and analysis of data are built into nearly every interaction a person has with a city agency. In many respects, these systems can serve the public good: automating benefits enrollment, tracking demographic needs, and helping agencies design programs more responsive to the people they serve. But for these systems to remain public goods, the city must confront the unprecedented scale of personal information it now holds. By digitizing many city services, the city now has information that is deeply intimate, such as biometric information and geolocational data, making it increasingly capable for the city to expose every facet of a person's life to inappropriate government scrutiny.

At the same time that city agencies have expanded their data infrastructure, the New York Police Department (NYPD or Department) has quietly embedded itself deeper into city systems. Over the last several years, police presence–both physical and digital–has expanded across agencies serving poor, unhoused, and disabled New Yorkers.[1] As a result, individuals who already face heightened risks of police harassment and violence are now made hyper visible to law enforcement across even more fronts. This entanglement reinforces the school-to-prison pipeline, intensifies the criminalization of poverty, and turns services meant to help New Yorkers into additional surveillance touchpoints.

As public defenders, we witness daily how pervasive data collection and surveillance technologies have also deteriorated the constitutional protections of the people we represent. Inaccurate Shotspotter alerts continue to trigger police responses and arrests without genuine probable cause.[2] Racially biased and error-prone facial recognition systems generate misidentifications that lead to wrongful stops, searches, and arrests. And because the machinery that produces these "leads" rarely enters a courtroom, the individuals subjected to these technologies and the public defenders representing them have no meaningful opportunity to challenge the integrity of evidence rooted in flawed surveillance tools. These technologies operate behind a veil, undermining the core constitutional protections that should protect every New Yorker.

More broadly, the city's growing surveillance infrastructure does not merely target individuals; it maps, categorizes, and criminalizes entire communities. The normalization of stripping low-income and working-class New Yorkers, and particularly New Yorkers of color, of their privacy rights must come to an end. Updating our data protection laws to match the conditions of the digital age is a necessary first step in reversing this trend.

Introduction 1335 and Resolution 783

For these reasons, BDS strongly supports Int. 1335. This legislation takes a critical step by expanding the definition of "personally identifying information" (PII) to reflect the realities of the digital age. Modern identification no longer relies solely on names, addresses, or traditional identifiers. Today, a person can be identified through countless data points: their faceprint, voiceprint, gait, geolocation history, app data, browsing patterns, and more. Int. 1335 recognizes that residents' digital identities are no different than one's physical identity and private effects, and therefore require the same level of protection. This is essential not only to prevent identity theft and commercial exploitation but also to ensure that public-service data collection does not become a gateway to expanded surveillance or unwarranted scrutiny.

---

[1] Katie Honan, Reuven Blau & Yoav Gonen, *NYPD Expands Role in Civilian Agencies as Feds Circle Top Cops*, The City (Sept. 11, 2024).

[2] Brooklyn Defender Services, *Confirmed: ShotSpotter Technology Increases Surveillance and Policing of Black and Latine New Yorkers, While Failing to Reduce Gun Violence: Analysis of Nine Years of Previously Undisclosed NYPD Police Data* (Dec. 4, 2024), https://bds.org/assets/files/Brooklyn-Defenders-ShotSpotter-Report.pdf

BDS also supports Resolution 783, which urges passage of New York State's Data Protection Act. Because data routinely flows between city and state systems, modernizing privacy protections at the state level is critical. Statewide consistency will help ensure that New Yorkers' sensitive information is safeguarded no matter which agency collects or stores it. This legislation is essential because porous information-sharing practices create conditions where data that is unnecessary or inappropriate for certain entities to possess nevertheless becomes available to them. Such leakage quietly erodes the right to privacy and expands the universe of actors with access to deeply personal information, increasing the likelihood of misuse or abuse. In New York City, this concern is especially urgent: as a sanctuary city, any gaps in our data-protection framework risk exposing sensitive personal information for the purposes of federal immigration enforcement.

Taken together, these measures begin the process of bringing New York's privacy laws into alignment with the technologies that shape modern life.

Beyond Data Protection, The City Must Limit the Use of Surveillance Tools That Gather Intimate and Unnecessary Personal Data

While Int. 1335 and Res. 783 take important steps toward modernizing privacy protections, the city cannot respect the fundamental right to privacy without also pulling back the invasive and discriminatory surveillance tools that undermine those very protections. Over the past decade, New York City's investment in police surveillance technology has far outpaced the establishment of modernized civil-rights laws that would recognize our digital identities as part of the "privacies of life" protected by the U.S. Constitution. The NYPD has spent more than a billion dollars on an array of powerful surveillance tools with little oversight or regulation. And even where the city has demanded transparency around data collection and surveillance, the Department has consistently sought to evade oversight and accountability. For instance, the NYPD routinely fails to provide comprehensive reporting on its own surveillance technologies as required under the POST Act. Further, the Department has pursued access and use of surveillance technologies through other agencies to avoid publicizing its surveillance activity. The recent revelation of its covert plan with the New York City Housing Authority (NYCHA) to obtain live access to thousands of residential CCTV cameras shows how readily the department is willing to circumvent public processes and democratic safeguards to expand its surveillance reach. These practices create new fronts of constitutional concern and expose New Yorkers to unchecked, technologically amplified policing that operates outside the limits the law intends to impose.

To protect people's constitutional right to privacy, we must not only protect the data the city collects, but must also prevent the city from collecting data it does not need, particularly when that data is discriminatory, inaccurate, or structurally incapable of responsible use.

Passage of Introductions 798 and 963 To Strengthen Data Protections

One of the clearest examples of why stronger data protections must be paired with limits on police surveillance is the NYPD's gang database. Oversight bodies, researchers, and community

members have long documented that the database overwhelmingly targets Black and Latine youth, many of whom have never committed a crime and have no verified connection to unlawful activity. The criteria now used to justify placement, such as alleged "self-admission" pulled from social media or proximity to others similarly labeled, are unscientific, pretextual, and racially coded. The result is not a tool for preventing violence or improving community health, but a set of dossiers on Black and brown New Yorkers that allows the NYPD to wait, watch, and criminalize people by association.

The harm of allowing police to gather and store intelligence in such discriminatory and inaccurate databases extends far beyond surveillance and street-level policing. For example, we've already seen ICE rely on false gang allegations to justify arrests and deportations. This demonstrates the breadth of the danger: a database built on bad information becomes a pipeline through which inaccurate labels travel to other agencies that wield enormous power over a person's liberty, family, and safety.

Even with legislation such as the New York Data Protection Act, which would help limit data leakage, the mere existence of this repository creates a completely unjustifiable risk. A person wrongfully labeled in the NYPD database as associated with a foreign gang could have that designation passed to ICE, placing them at risk of detention, deportation, or removal to a country where they may face persecution or human rights abuses.

We do not need this database, and we have ample documentation that it is inaccurate, discriminatory, and easily abused. The NYPD has demonstrated a willingness to bend or break rules to access and share information, and there is no credible way to regulate a system built on such deeply flawed foundations. The time has urgently come to abolish the gang database in its entirety. City Council must pass Int. 798 to eliminate this harmful and dangerous system.

The concern over excessive surveillance and data gathering extend beyond NYPD surveillance and into the broader criminal legal system. People are losing ownership over some of the most intimate aspects of their identities. Systems like Securus, the jail call recording software used in New York, does far more than simply record calls. The AI-enabled software extracts and stores voiceprints, a form of biometric data that would rightly fall under the expanded definition of personally identifying information contemplated in Int. 1335. Crucially, it is not only incarcerated people whose identities are captured: any family member or friend who calls into a jail has their unique voiceprint taken, even when they are not under investigation. Securus also integrates tools such as Securus Threads[3], which allow correctional staff to analyze the social networks of incarcerated individuals and generate maps of those networks inside and outside of prison. Individuals calling their loved ones may have data from those calls shared with the NYPD, raising the risk that they will be surveilled based on their association with an incarcerated person, in violation of their right to privacy and their First Amendment associative freedoms. This means that people engaging in the deeply human act of supporting someone in custody, something shown to reduce recidivism and improve outcomes, may instead find themselves

[3] Securus Technologies, *THREADS — Investigative & Corrections Analytics*, https://securustechnologies.tech/securusthreads/

under police scrutiny or harassment. This information should not simply be protected as personal information or regulated under a data protection act - it should not be gathered at all. For these reasons, in order to protect New Yorker's digital identities and privacy, City Council must also pass Int. 963, the End Community Correctional Surveillance (ECCoS) Act, to end the invasive and inappropriate surveillance of incarcerated people and their loved ones.

Conclusion

As technology increasingly shapes the operations of government and the daily lives of New Yorkers, it is essential that our laws reflect both the risks and responsibilities of this moment. Our city urgently needs expanded data protection laws, limitations on discriminatory surveillance tools, meaningful oversight over the development of algorithms used by city agencies, and so much more. These changes in our legal framework are not only matters of good governance, they are necessary to preserve the constitutional rights and civil liberties that form the foundation of a democratic city.t

Int. 1335 and Resolution 783 modernize the baseline protections residents need in an era of pervasive digital information collection. Ints. 798 and 963 go further by addressing the systems that pose immediate, well-documented harms to Black, brown, immigrant, and low-income New Yorkers, and by ensuring that deeply personal data is not collected or misused in ways that undermine safety, privacy, or due process.

We thank the Committees on Technology and Civil and Human Rights for their commitment to addressing these issues. If you have any questions, please do not hesitate to contact Jackie Gosdigian, Senior Policy Counsel, at jgosdigan@bds.org.

Good afternoon Chairs, Council Members. My name is Clayton Banks, CEO of Silicon Harlem. Thank you for the opportunity to speak about privacy protections in our rapidly evolving digital world.

For more than a decade, my organization has worked across Upper Manhattan to help residents embrace technology. However, people will only embrace innovation if they trust it. Privacy is not separate from innovation, it is the foundation that makes innovation possible.

TESTIMONY

Int. 1335 – Modernizing the definitions of identifying and private information

This update is essential. Today, identifying information includes far more than names and numbers, it's biometrics, location signals, device identifiers, patterns of movement, and AI-generated profiles.
My opinion: NYC must modernize these definitions so residents are protected from invisible digital harms.

Int. 1340 – Gendered impact assessments for AI

AI cannot serve the public if it unintentionally harms the public.
Bias often appears at the intersections, gender, race, disability, age.
My view: This bill is a meaningful step toward accountability and fairness.
Neutral view: Impact assessments also increase trust, which strengthens adoption.

Int. 1367 – A top-level domain requirement for city websites

Many residents, especially seniors, struggle to distinguish legitimate city sites from scams.
Opinion: A secure, consistent domain system improves safety and confidence.
Neutral view: It also reduces confusion across agencies.

Res. 0783 – Supporting the New York Data Protection Act

Data is the new infrastructure. And communities with the least protection face the greatest risk.
Opinion: Strong data rights empower New Yorkers who have historically been over-surveilled and underprotected.
Neutral view: Statewide standards offer clarity for businesses and government alike.

Res. 1062 – Right to Your Own Image Act

In the age of deepfakes and generative AI, this is critical.
Every New Yorker deserves ownership of their likeness and voice.
Opinion: This bill protects dignity and prevents misuse.
Neutral view: It also gives creatives and companies clear, predictable rules.

My idea is - Build Harlem as a “Digital Rights Zone”

A partnership that positions Harlem as a **model neighborhood** for:

- AI fairness
- privacy protections
- safe digital infrastructure
- deepfake detection education
- safe city websites and verified digital communication

Opportunity: Harlem becomes the pilot neighborhood for NYC’s privacy protections.

Closing

Across NYC, I see every day that communities welcome new technology when they know **their rights travel with them**. Privacy, transparency, and accountability are not barriers. They are the backbone of a healthy digital society.

Thank you for your leadership.

Clayton Banks
Silicon Harlem
mr.banks@siliconharlem.com

SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (212) 518-7573

STATEMENT OF
ALISSA JOHNSON, LEGAL FELLOW
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT ("S.T.O.P.")

BEFORE THE COMMITTEE ON CIVIL AND HUMAN RIGHTS AND THE COMMITTEE ON TECHNOLOGY,
NEW YORK CITY COUNCIL

PRIVACY PROTECTIONS IN THE DIGITAL AGE

PRESENTED
December 8, 2025

Good afternoon, members of the New York City Council Committees on Technology and Civil and Human Rights. Thank you for organizing this important hearing. The Surveillance Technology Oversight Project ("S.T.O.P.") is a New York-based civil rights and anti-surveillance group that advocates and litigates against discriminatory surveillance.

1. Int 1335-4420 – Definitions of identifying information and private information

STOP's position is that IP and MAC addresses already fell within the definition of section 23-1201 of the admin code, as "information that may be used on its own or with other information to identify or locate an individual." But, including these identifiers within the section's definition is nevertheless useful for purposes of clarity. STOP supports Int 1335-4420.

2. Res 1062-2025 – Right to Your Own Image Act (A.3924)

STOP maintains that AI generated deepfakes already fell under the civil rights law's definition of "likeness." Nonetheless, as with Int 1335-4420, including them explicitly can only help. The right of publicity is an important check on data brokers, and strengthening the right helps New Yorkers and organizations like STOP hold data brokers accountable for violating our rights.

3. Int 1340-2025 – Interagency taskforce and reporting on a gendered impact assessment of artificial intelligence

We recognize the council's efforts to address the critical issue of gender discrimination in algorithmic decision-making. However, we have concerns that this amendment to the administrative code will be ineffective in addressing the issue. As written, the proposed taskforce would not account for algorithms using proxies for gender, rather than gender itself, as input variables. This reporting requirement will miss most algorithmic tools that *do* discriminate on the basis of gender, as such tools may not explicitly use gender itself as an input. Only auditing algorithms that use gender itself as an input may also provide cover for algorithms that have discriminatory impacts without explicitly considering gender—giving them the veneer of neutrality without the rigor of an audit.

Additionally, the introduction does not specify the mechanism of "analysis" to be performed in evaluating the tool. STOP is concerned that existing bias auditing methods can be ineffective in identifying gender bias, further limiting the taskforce's effectiveness.

STOP supports the establishment of a task force to ensure algorithmic tools used by NYC agencies do not discriminate on the basis of gender—but such a task force would be more effective if it analyzed all tools used in hiring, as reported under section 3-119.5(c), for disparate effects based on gender, rather than only those listed under the new reporting requirement as specifically using gender as an input factor. STOP specifically supports the introduction's **public reporting requirement**, which would allow civil society to supplement the task force's work with independent analysis of reported algorithms' discriminatory impacts.

4. Res 0783-2025 – Enacting the New York Data Protection Act (S. 4860)

STOP commends the council on the laudable goal of addressing ever-increasing government data collection and information sharing across agencies. However, STOP has concerns that the Data Protection Act (DPA) as written fails to address the forms of data sharing which put vulnerable New Yorkers most at risk: unfettered, warrantless data sharing with law enforcement.

Overall, STOP feels that the DPA largely echoes the protections of New York's existing Personal Privacy Protection Law (PPPL), and that the changes made under the DPA would be more effective as amendments to that law. The DPA does extend disclosure requirements to local agencies in addition to the state agencies covered under the PPPL, and imposes a (relatively weak) data deletion requirement, both changes that STOP supports. However, the DPA's actual knowledge standard for imposing liability when an agency's contractor misuses data is too stringent, and, in combination with the DPA's lack of a private right of action, would functionally prevent recovery for careless handling of New Yorkers' data.

The DPA does include some protections against data sharing between agencies, but these protections still leave loopholes for sharing with law enforcement, putting New Yorkers' privacy at risk. The DPA's § 86 prohibits sharing with another government entity **unless** "such information is crucial to the performance of such other government entity or contractor's duties"—a requirement that law enforcement agencies can easily argue is satisfied whenever they seek access to our data. A warrant requirement, by contrast, would require law enforcement to specify what information they are seeking, and why.

STOP agrees with the council that excessive data sharing by government agencies poses a threat to New Yorkers' civil liberties. However, we feel that this issue would be better addressed by extending the PPPL to municipalities and closing its loopholes by preventing warrantless sharing of information with law enforcement, through a bill like S.4044-2023 (which has not yet been introduced for the 2025-2026 session).

Thank you for the opportunity to testify today.

Testimony by Cynthia Conti-Cook, Director of Research and Policy

Presented before the

New York City Council Committees on Technology and Civil & Human Rights

Oversight Hearing on Privacy Protection in the Digital Age

December 8, 2025

The Collaborative Research Center for Resilience (CRCR) nurtures futures that build towards a vibrant democracy and a world where we can all thrive. We bring together collaborators across issue areas—locally and transnationally—to research technologies that shape the governance of our day to day lives. We focus on how to increase participatory engagement and design in government implementation of technologies. We design locally appropriate solutions by expanding collaborations with and across stakeholders.

We testify to raise awareness about recent developments in data sharing, privacy protocols, and pending state legislation pushed by the outgoing administration over the past three years that undermine New Yorkers' expectations of privacy, articulated by the Identifying Information Local Laws 245 and 247 passed in 2017. These laws articulated an expectation that personal identifying information collected for the purposes of accessing city services would be protected by agency privacy officers from suspicion-less seizure and corporate sale.

We support the amendments to the Identifying Information Law in Intro 1335 and we continue to call for the Council to revisit the list of agencies exempted from privacy protections and reporting, specifically NYCHA, the NYPD, and other law enforcement. The expansion of deference to the NYPD in the 2025 amendments to the Citywide Privacy Protocols also supports revisiting the exceptions granted them–the new

amendments essentially direct agency privacy officers to consider any request made by an NYPD officer legitimate, even when the agency privacy officer is directed to assess the credibility of demands made in anticipation of crime and not based on individualized suspicion.

We support Resolution 783 but also urge the Council to address the loopholes presented by interagency data sharing and ask that the Council also pass a resolution calling on the legislature to oppose efforts like the One City Act because of how it specifically undermines the intent behind the Identifying Information Law of 2017.

Finally, as revealed at the end of the Chief Privacy Officer's testimony, the placement of the Chief Privacy Officer under the Office of Technology and Innovation has mollified its capacity to properly and urgently respond to breaches of public information and trust.[1] That role should be returned to its previous placement under Counsel's office, where the liability of privacy breaches is more properly understood.

Historical Background of Identifying Information Laws 245 and 247 of 2017

The suite of data privacy laws contained in Chapters 12 of the City Charter were passed in 2017 as part of an effort to "protect personal information held by the City."[2] Championed by then-Speaker Melissa Mark-Viverito and then-Council Member Jumaane Williams, local laws 2017/245 and 2017/247 established defined limits on when and how agencies could disclose personal information and created agency privacy officers to ensure compliance with those limits. It is important to remember the historical context in which the initial privacy protections were enacted. In 2017, as the first Trump administration initially threatened our immigrant communities and local politicians sued to access the identity paperwork for cardholders of the new IDNYC, the City Council passed privacy protections on behalf of all New Yorkers in relation to the identifying information they share to access city goods and services.[3]

---

[1] https://nyc.legistar.com/MeetingDetail.aspx?LEGID=22011&GID=61&G=2FD004F1-D85B-4588-A648-0A736C77D6E3

[2] New York City Council, *Council to Vote on Legislation to Protect Personal Information and Create a Comprehensive Privacy Policy for the City of New York* (Nov. 16 207), https://council.nyc.gov/press/2017/11/16/1546/

[3] *New York City Should Keep ID Data for Now Judge Rules*, The New York Times, Dec. 12, 2016, https://www.nytimes.com/2016/12/21/nyregion/new-york-city-should-keep-id-data-for-now-judge-

Not only were these laws intentionally designed to keep private information out of the hands of federal immigration enforcement agencies like ICE, but they were also meant to protect against abuse and mishandling of personal information by New York City agencies and employees.[4] Through these laws, New Yorkers clearly recognized that protecting broad access to safety net services for all who need them keeps all of us more safe.[5]

These and other recent efforts to strengthen privacy protections are just the latest in a series of struggles to respond to the corrosive corporate surveillance technologies that the government has increasingly procured to police, punish, and cut off people who access city services.[6] As the Chair of the Civil Rights Committee reminded the Chief Privacy Officer at the hearing on December 8, 2025 as an example of this, people seeking city services for victims of crimes have been denied access based on NYPD data about their group affiliations. Multiple mayoral administrations have increased government reliance on corporate technology. Going at least as far back as the Bloomberg administration's executive order in 2008 to consolidate private information as part of the HHS-Connect initiative[7], through programs like Worker Connect in 2010[8], LinkNYC in 2016[9], Big Apple Connect in 2022[10] and continuing past the launch of MyCity in 2023[11], New York City has relied on expanded data collection and disclosure

---

rules.html

[4] New York City Council, *Speaker Melissa Mark-Viverito Delivers 2017 State of the City Address* (Feb. 16, 2017), https://council.nyc.gov/press/2017/02/16/1370/

[5] *Supra* note 14, (statement of Jumaane Williams).

[6] New York City Council, *City Council Passes Expanded POST Act Legislative Package to Strengthen Transparency and Oversight of NYPD Surveillance Technology* (Apr. 15, 2025), https://council.nyc.gov/amanda-farias/2025/04/15/city-council-passes-expanded-post-act-legislative-package-to-strengthen-transparency-and-oversight-of-nypd-surveillance-technology/; *see also* https://www.nysenate.gov/legislation/bills/2025/S4860 (bill to establish the New York Data Protection Act)

[7] City of New York. "EXECUTIVE ORDER No. 114," (Mar. 18, 2008), https://www.nyc.gov/html/om/pdf/eo/eo_114.pdf

[8] Allon Yaroni, *Worker Connect: A Process Evaluation of a New York City Data Integration System*, Vera Institute of Justice (Nov. 2015), https://www.nyc.gov/assets/opportunity/pdf/workerbriefs7c.pdf ; https://www.nytimes.com/2011/06/17/nyregion/promise-and-concern-for-vast-social-services-database-on-citys-neediest.html?searchResultPosition=1

[9] NYCLU, *LinkNYC is a Privacy Disaster. Here's Why* (July 27, 2023), https://www.nyclu.org/commentary/linknyc-privacy-disaster-heres-why

[10] Office of Technology and Innovation, *Big Apple Connect*, https://www.nyc.gov/content/oti/pages/big-apple-connect

[11] Office of the Mayor, *Mayor Adams Launches First Phase of MyCity Portal* (Mar. 29, 2023),

of personal identifying information in its delivery of social services. As a result, city agencies have increasingly leveraged private contractors and data sharing agreements, even when it requires defying City Council.[12]

Despite the guardrails put in place by the 2017 privacy laws, city agencies have signed wide-ranging agreements to share data, as encouraged by the Citywide Privacy Protocols. One such agreement was reached in 2023 between the Office of Technology and Innovation, the Administration for Children's Services, the Department of Homeless Services, the Department of Education, and the Human Resources Administration for the purpose of consolidating personal information as part of MyCity.[13] For example, this agreement allowed OTI to disclose information in response to a demand without any of the responsibility of agency privacy officers to comply with notice to the subjects of those demands or other legal reviews.

The One City Act

Because these agreements are on shaky legal ground under the current Charter, the administration has repeatedly pushed for legislation called the One City Act as an after-the-fact blessing from Albany that would permit the continued expansion of data sharing, consolidation, and disclosure across city government.

In 2024, Assemblyman Alex Bores—a former executive of the data-mining and surveillance giant Palantir—introduced the "One City Act" into the New York State Assembly.[14] Four other assembly members co-sponsored the One City Act's introduction: Jo Anne Simon (a former disability rights lawyer), Maritza Davila (a former community organizer), Rebecca Seawright (a former Chair of the Feminist Press at

---

https://www.nyc.gov/mayors-office/news/2023/03/mayor-adams-launches-first-phase-mycity-portal-easily-help-new-yorkers-check-eligibility

[12] Zachary Groz, *Adams Locks In Big Apple Connect Through 2028, One Day Before Oversight Hearing* (Sep. 29, 2025), https://nysfocus.com/2025/09/29/adams-big-apple-connect-renewal

[13] Office of Technology and Innovation, *MyCity Data Sharing Agreement - Childcare* (Mar. 21, 2023), https://www.nyc.gov/assets/oti/downloads/pdf/about/mycity-data-sharing-agreement.pdf

[14] Wendy Blake, *One-time Exec at Controversioal Tech Giant Enters Dem Assembly Race, Wants to Use Cyber Savvy to Protect NYC*, EAST SIDE FEED (Mar. 4, 2022), https://eastsidefeed.com/politics/one-time-exec-at-controversial-tech-giant-enters-dem-assembly-race-wants-to-use-cyber-savvy-to-protect-nyc/; Palantir routinely supplies services and information to federal immigration enforcement and has deep ties to agencies like the CIA; Assemblyman Bores has publicly disavowed Palantir's cooperation with ICE and cites it as a major reason why he left the company.

CUNY), and Tony Simone (a former Director of Community Outreach for the NYC Council).[15] The One City Act was referred to the Cities Committee of the Assembly in 2024, where it remained permanently.

A month later, Senator Andrew Gounardes—former counsel to Eric Adams for five years—introduced a textually identical version of the One City Act in the New York State Senate.[16] Two other senators sponsored the bill: Luis Sepúlveda (a former assemblyman) and Robert Jackson (a former school board president and NYC Councilman). It was referred to the Cities Committee of the Senate in 2024 where it languished in a similar fashion to its Assembly counterpart.

Unlike the original Assembly version, Gounardes's Senate version of the One City Act came with two key legislative justifications: bolstering the outgoing administration's Subway Safety Plan and the MyCity portal.[17]

One of the central pillars of that particular Subway Safety Plan was increased deployment of NYPD officers in both subway cars and on platforms to forcibly remove and involuntarily hospitalize New Yorkers suffering from psychiatric crisis or homelessness. By making it easier for city agencies to disclose private personal information to the NYPD, the One City Act is designed to justify police use of force and abet the tracking, identification, and surveillance of individuals that the NYPD wants out of the subway system. The vast amounts of data that the One City Act makes available to police can and will be used to justify the forcible removal, forced hospitalization, and forced treatment of New Yorkers, such as through Mental Hygiene Law 9.60.[18] With access to information about nearly every facet of an individual's life, the police will have no shortage of ways to manufacture reasons to arrest, forcibly seize, remove, and subsequently deny benefits and services to individuals stopped on the subway.[19]

---

[15] https://www.nysenate.gov/legislation/bills/2023/A9642

[16] https://www.nysenate.gov/senators/andrew-gounardes/about

[17] https://www.nysenate.gov/legislation/bills/2023/S9124

[18] NYCLU, *Statement of Beth Haroules Before the Assembly* (Feb. 27, 2007) (describing the harm of involuntary treatment and the gross racial disparities in the enforcement of mental health laws), https://www.nyclu.org/resources/policy/testimonies/testimony-extending-kendras-law

[19] Ana Ley, *Citing Safety, New York Moves Mentally Ill People Out of the Subway*, NEW YORK TIMES (May 10, 2024), https://www.nytimes.com/2024/05/10/nyregion/nyc-subway-mental-health-homeless.html

The One City Act was also designed to expand the scope of data sharing for the disastrous MyCity portal.[20] MyCity has funneled tens of millions of taxpayer dollars to private tech contractors while endangering the security of New Yorkers' personal information and providing few meaningful services.[21] The One City Act would only exacerbate the problem by making it easier than ever for the Mayor's office to unsafely collect and store personal data, as well as to disclose personal information to private contractors without safeguards or oversight.

Given the incoming administration's pledge to increase "interagency coordination," including with the NYPD, and to consolidate social services agencies into a new "Department of Community Safety," there is a dire need to ensure privacy for New Yorker's most sensitive information.[22] The One City Act will do the opposite by unleashing the NYPD and benefits agencies to scrutinize and weaponize people's own data against them.

In 2025, a nearly identical One City Act was re-introduced to the Assembly by Alex Bores and sponsored this time only by Maritza Davila. It contained a single minor difference in wording, but no clear substantive changes. It was referred to the Cities Committee on February 24, 2025, where it remains.

The One City Act was also re-introduced to the New York State Senate in 2025, again by Andrew Gounardes. In addition to prior sponsor Robert Jackson, this bill was co-sponsored by Leroy Comrie (a former NYC Councilman). It was first referred to the Cities committee on January 27, 2025, but was later moved to the Senate Committee on Internet and Technology on May 20, 2025, where it stayed.

During its reintroduction, Senator Gounardes once again provided a legislative justification for the bill. The new justification removed the paragraph detailing the Act's possible uses regarding the Subway Safety Plan and MyCity Portal, but otherwise

---

[20] Zachary Groz, *How Eric Adams's MyCity Portal Became a $100 Million Question Mark*, NEW YORK FOCUS (March 19, 2025), https://nysfocus.com/2025/03/19/mycity-eric-adams-child-care

[21] Cythnia Conti-Cook and Ed Vogel, *MyCity, Inc: A Case Against "Compstat Urbanism"* (New York: Surveillance Resistance Lab, March 18, 2024), https://surveillanceresistancelab.org/featured-work/mycity-inc-a-case-against-compstat-urbanism/

[22] https://www.zohranfornyc.com/platform (full report accessible by opening tab labeled "The Department of Community Safety" and clicking hyperlink labeled "Read our full proposal here")

remained unchanged.[23] Despite this formal change in legislative justification nothing in the actual text of the bill was altered. Thus the One City Act, as before, will increase policing and the disclosure of private data to the harm of New Yorkers.

NYC Administrative Code, Identifying Information Laws

Sections 23-1201 through 23-1205 of Chapter 12 of the New York City Charter are the city's current municipal privacy laws regarding interagency data sharing.[24] These sections function alongside the rules for how agencies handle security breaches and dispose of private information supplied in Sections 10-501 through 10-504 of Chapter 10 and the general power of the Mayor to establish an office of information privacy described in Chapter 1, Section 8, subdivision h, to create an overall framework for how New York City handles personal private information. These laws would be displaced by the One City Act, leaving New Yorkers without any protection of their private data except the lenient requirements of the One City Act.

The One City Act would impact the New York City Administrative Code sections related to the Identifying Information Law in the following ways:

Section 23-1201

Section 23-1201 supplies key legal definitions for terms like "Human services," "Identifying information," and "Routine collection or disclosure." Its definition of "human services" is borrowed from another part of the Charter—Section 6-129 of Chapter 1 of Title 6—and includes all manner of social services like "day care," "housing and shelter assistance," "medical services," and "employment assistance services." Conspicuously absent from this definition is any mention of crime, policing, or public safety services.

The One City Act's new definition (which, as discussed, explicitly mentions "crime" in the context of defining human services agencies) would therefore undercut the intent of the City Council in 2017 to keep data sharing and disclosure confined to agencies and contractors whose mission is to actually supply social services, not criminal law enforcement agencies like the NYPD.

---

[23] https://www.nysenate.gov/legislation/bills/2025/S3392

[24] https://codelibrary.amlegal.com/codes/newyorkcity/latest/NYCadmin/0-0-0-42878

Section 23-1201 also defines “routine collection or disclosure” of information. While agency privacy officers are currently allowed to form data sharing agreements about collections and disclosures classified as “routine,” they are by law limited to sharing information “that is made during the normal course of city agency business and furthers the *purpose or mission of such agency*.”[25]

By contrast, the One City Act permits agreements whenever there is a “government function to assist individuals.” While the current regulations are far from perfect, they at least expect and require that the use of private information be done in furtherance of an agency’s central mission, and not just because the agency can paint a colorable picture that someone somewhere will potentially benefit from it.

Section 23-1202

Section 23-1202 puts forward substantive restraints on agency data sharing. For instance, Section 23-1202(c) removes city agencies’ ability to disclose personally identifying information, *including to other city agencies*, without first securing the approval of their privacy officer. Additionally, an agency must be able to show that each disclosure either (1) is authorized by the individual whose information it is, (2) “furthers the purpose or mission of such city agency,” or (3) is otherwise required by law.

As discussed above, the second of those exceptions, furthering the mission of the agency, is already quite broad, but the One City Act still significantly eclipses it in scope. The One City Act would essentially remove the requirements of Section 23-1202(c) entirely, as an agency can practically always claim to be assisting individuals or managing the provision of services.

Furthermore, the One City Act allows for a continuous transmission and exchange of data once an agreement is signed. Section 23-1202, by contrast, generally enforces a case-by-case approach to data sharing by requiring that an agency’s privacy officer sign off on every disclosure, even if it meets all the other stated requirements.

Thus, the One City Act would allow city agencies to routinely share massive volumes of data that had previously been too onerous to disclose. Rather than picking and choosing to release only the data that is most important to their mission, agencies would

[25] Charter § 23-1201

likely begin forming broad data-sharing pacts that would disclose more information than otherwise necessary, if for no other reason than their own convenience.

The one-time nature of One City Act agreements may also reduce oversight, as agencies will have little incentive to review either the terms of the agreement itself or the data actually being shared under it once it is in place. Agencies already classify a distressing amount of information as “routine” without much consideration, and the One City Act would only exacerbate this issue. Even if an agreement appears to include sufficient protections, agencies are unlikely to review the disclosed data for compliance with those terms given the amount of time it would take, leaving New Yorkers’ private information to be tossed between city agencies without sufficient review or oversight.

Section 23-1203

Section 23-1203 of the City Charter defines minimum requirements for the policies set by the city’s chief privacy officer (who is appointed by the Mayor) to ensure a basic level of security for New Yorkers’ personal information. While the chief privacy officer has a great deal of latitude in setting policies related to the collection, storage, and transmission of private data, Section 23-1203 imposes important limiters on them (such as requiring anonymization of identifying information where possible). Importantly, several of the requirements imposed by Section 23-1203 incorporate the general prohibitions on disclosing personal information detailed in Section 23-1202.

Since the One City Act would effectively eviscerate Section 23-1202, it would also leave many of Section 23-1203’s requirements nullities. The result would be to give the city’s chief privacy officer unfettered discretion to decide how protective agreements made under the One City Act would have to be, totally freed from any minimum restriction or guardrails. This would represent a significant erosion of privacy guarantees for the people of New York as well as an expansion of unchecked Mayoral authority over the personal information of millions of people.

Section 23-1203(3), meanwhile, places limits on city agencies’ ability to share data with third parties equivalent to the requirements of 23-1202(c). As such, agencies currently have to enter into signed agreements with third parties (such as vendors) verifying compliance with privacy guidelines for both anticipated and potential future use before

disclosing any private information. Moreover, unless classified as “routine,” agencies must do this *each time* they disclose information to a third party.

The One City Act, however, permits long-term data sharing agreements to be with either an agency “or agent thereof.” “Agent” is defined in turn as a person who acts “on behalf of or at the direction of” an agency. This definition is once again extremely permissive, granting agencies wide latitude to delegate and direct private contractors to act on their behalf while handling huge amounts of private personal information. The MyCity project stands as proof of the dangers—both to finances and privacy—of allowing long-term agreements with private technology contractors to operate without consistent oversight.[26] The last thing we need is for the One City Act to make those kinds of agreements even more common.

It is critical for this committee to carefully examine the police and corporate influence on all technology procurement, contracting, and personnel decisions made throughout all city agencies in the past four years under the outgoing administration. The number of NYPD officers placed in agencies like the Office of Technology and Innovation, Parks, Sanitation, and many other agencies with the explicit intent to conflate how the city policies regulations with how the NYPD polices crime endangers the safety of New Yorkers seeking safety net services and access to public goods like the identifying information of IDNYC cardholders.

Impact of One City Act on New York City Identifying Information Laws

The One City Act sets out a series of permissive regulations for the formation of data-sharing agreements between municipal agencies of New York City.[27] Specifically, it empowers any municipal agency to disclose private personal information that would otherwise be barred by New York law for any purpose related to “[b]enefits, services and care coordination.” That phrase repeats throughout the bill with non-exhaustive definitions included: “Benefits” includes *any* assistance or resources provided for the fulfillment of basic needs (e.g. food, shelter, education, health care); “Services” means *any* government function performed to assist individuals; and “Care coordination” refers to *any* coordination or case management related to the provision of benefits or services.

---

[26] *See* supra, note 10.

[27] Supra, note 13.

Despite the One City Act's misleading description of these definitions as "limited," they are in fact so broad that they encapsulate virtually every conceivable agency action or program. Far from just serving public health and safety, the One City Act would effectively remove any constraints on the purposes for which government agencies could disclose people's private information.

In addition to the definitions provided above, the One City Act also defines "Human Services Agency" to include any agency that delivers services to improve health or welfare, and explicitly includes "crime" as an example of such a service. The obvious but alarming consequence is that the One City Act classifies the NYPD as a "Human Services Agency." Not only does this permit the NYPD to conduct research studies using all manner of shared data, it is also evidence that combating or prosecuting "crime" is being smuggled into the Act's general definition of "[b]enefits, services, and care coordination." In effect, this means that the One City Act would allow the NYPD to disclose or request the disclosure of private information virtually without restriction, as their purpose will always be in some way related to "crime."

An illustrative example of how the One City Act functions was included in Senator Gounardes's initial justification for the bill when it was introduced to the New York State Senate. New York Mental Hygiene Law Section 33.13 is a law which bars the release of confidential medical records in most circumstances.[28] While Mental Hygiene Law 33.13 contains a multitude of specific carve-outs and exceptions tailored to various circumstances, it has no categorical allowance for disclosure for the purpose of providing benefits or services. The One City Act would create just such an allowance, thus significantly enlarging the ability of agencies to share these types of restricted records. By creating a generalized justification (the provision of benefits and services), the One City Act changes the default posture towards disclosure of personal information. Information may now *presumptively* be disclosed, whereas before it was presumed that such information was confidential and could not be disclosed except in narrow circumstances where the need to do so was pressing. It should be noted that all other state laws resembling the Mental Hygiene Law would see a similar erosion of privacy constraints.

---

[28] https://www.nysenate.gov/legislation/laws/MHY/33.13

Data-sharing agreements under the One City Act are subject to three important limitations. First, federal law may preempt the ability of city agencies to share data amongst themselves. Second, the data sharing agreements may not include records required to be sealed under New York law (such as conviction records sealed under the Clean Slate Act). Third, the Act does not authorize data sharing for the purpose of investigating legal offenses as defined under the New York Penal law.

Finally, the One City Act also includes certain requirements for the agreements formed between agencies. Interagency agreements must be approved by legal counsel and the agency's chief information security officer, limit access to the shared data to employees who require it to fulfill job functions, describe what data will be shared and by what methods, include the stated purpose why such information is required, prohibit redisclosure or publication of the information, and impose requirements for secure transmission and storage of the information no less stringent than the standards set by the city's chief cyber security officer.

Though these requirements sound like they reduce the ability of agencies to share information (and may in fact do so to a limited extent), the long-standing nature of agreements under the One City Act means that agencies only really need to fulfill these requirements at the time they sign the initial agreement. After such an agreement is signed, however, agencies can continuously disclose personally identifying information without ever needing to provide updated justifications or perform assessments to ensure compliance with the terms of the agreement.

As is made clear in the next section, this would substantially increase the amount of data transmitted between agencies and private third parties compared to the current regulations covering New York City agencies, which at least facially expect regular assessments and approvals of disclosures of private information. Even with its seemingly strict requirements, then, the effects of One City would be to significantly broaden the purposes for which private data can be disclosed while also increasing the amount of data transmitted and reducing agency accountability.

CONCLUSION

The One City Act is the latest in a long line of efforts to undermine the security of New Yorker’s private information in the guise of delivering critical social services. It would not

only allow agencies to more easily disclose data between themselves and third parties but also provide legal cover for existing agreements that test the boundaries of existing privacy laws. The One City Act would adopt definitions so broad and generally applicable as to effectively remove any barriers to data sharing.

In so doing it would abrogate existing municipal laws—laws passed with great care and intention by City Council—that require particularized review and authorization for disclosures of identifying information and replace them with a scheme in which a single agreement can authorize years of endless disclosures without meaningful oversight. The One City Act would leave the safety of private information at the unchecked whims of the Mayor and the city's chief privacy officer by eliminating legal minimum requirements for agency collection, storage, and transmission of data.

Finally, the One City Act would create incentives and authorize the NYPD to create a massive consolidated database of private information because it considers policing a type of human service, as if it was equivalent to benefits, day care or housing assistance. Unless reigned in, that database would likely be used to implement policing strategies for “community safety” that could readily be weaponized by future administrations against the same communities that pro-social policies seek to support.

WRITTEN COMMENTS OF WIRED BROADBAND, INC.

By Odette J. Wilkens

President & General Counsel

at Committee on Technology Hearing

December 8, 2025, 1pm

I am Odette Wilkens, President & General Counsel of Wired Broadband, Inc., a non-profit advocating for safe communications infrastructure, and am Executive Director of the NYC Alliance for Safe Technology. I have been a technology transactional attorney for over 20 years having represented multinational corporations. I also recently served on the Federal Communications Commission's Communications, Equity and Diversity Council (CEDC), along with Chair Gutierrez and representatives of equity organizations from across the country.

There's a safe way of deploying communications infrastructure, and an unsafe way, in terms of privacy and cybersecurity. We are deploying it in NYC in an unsafe way. We are commenting on the following bills: Int. 1335, 1340, 1367,0783 and 1062.

There are significant privacy and cybersecurity vulnerabilities in connection with the 5G rollout in NYC. Our recommendation is that there should be no further 5G deployment until privacy and security can be assured for NYC residents. 4G and 4G LTE provide more than adequate coverage without the privacy and cybersecurity vulnerabilities of 5G.[1]

[1] NYC is not under federal preemption to deploy 5G as 5G is not covered by the Telecommunications Act of 1996 (TCA), see *ExteNet Sys. v. Vill. of Flower Hill*, No. 19-CV-5588-FB-VMS, 9-10 (E.D.N.Y. Jul. 29, 2022). The court ruled that, under the TCA, local governments have authority over the number and placement of wireless facilities, and to deny the irresponsible placement of wireless facilities. Therefore, the FCC rule that makes the deployment of 5G automatically preemptible under the TCA is erroneous, does not comply with the TCA and does not apply to NY jurisdictions.

Privacy Vulnerabilities

There was concern at Manhattan Community Board 8 that 5G Towers would track their children's locations. 5G uses a beam-forming technology that tracks your cell phone.[2] Will our children's locations be tracked?

The privacy policy in the City's franchise agreement with CityBridge states that CityBridge does not support a "do not track" function,[3] therefore, users' (and children's) online activities can be tracked. CityBridge also states that, although they "do not collect information about your precise location," they "can determine your general location" when you are using their services.

OTI had stated that personal information would not be exploited by CityBridge,[4] but the privacy policy states that third party providers would be managing email addresses without a stated obligation that those providers would maintain confidentiality and would also not exploit personal information.[5] In addition, CityBridge states that it "cannot guarantee against access" to personal information by unauthorized third parties, and that "[t]he security of your data transmitted" using their services "is at your own risk."[6]

CityBridge in its presentation to MCB8 denied that it had any affiliation with Google. But there was an association with Alphabet (parent of Google with its massive personal data collection[7]), an investor in one of the companies that formed a consortium with CityBridge

---

[2] RF Coherency technology drives 5G RAN innovation, June 22, 2022, https://www.rcrwireless.com/20220622/5g/rf-coherency-technology-drives-5g-ran-innovation-reader-forum; see also, What is 5G?, https://cdn.shopify.com/s/files/1/0266/5411/3837/files/5G_White_Paper_-_EMR_Australia.v1.1.pdf?v=1613734363.

[3] CityBridge Privacy Policy, Exhibit 2 to Franchise Agreement between Department of Information Technology and Innovation (DoITT) and CityBridge, LLC, undated and unexecuted version, p. 4, https://www.nyc.gov/assets/oti/downloads/pdf/linknyc-franchises/linknyc-public-communications-structure-franchise-exhibit-2.pdf.

[4] See, e.g., Public Design Commission Meeting 12-13-21 Video (starts at 2:00), https://www.youtube.com/watch?v=nTBM95YcdF8.

[5] CityBridge Privacy Policy, Exhibit 2 to Franchise Agreement between DoITT and CityBridge, LLC, undated and unexecuted version, pp. 3-4, https://www.nyc.gov/assets/oti/downloads/pdf/linknyc-franchises/linknyc-public-communications-structure-franchise-exhibit-2.pdf.

[6] Id.

[7] Google faces $5 billion lawsuit in U.S. for tracking 'private' internet use, June 2, 2020, https://www.reuters.com/article/us-alphabet-google-privacy-lawsuit/google-faces-5-billion-lawsuit-in-u-s-for-tracking-private-internet-use-idUSKBN23933H.

for the buildout of LinkNYC, the predecessor to Link5G. Although this was a prior association, there is still the concern over the potential tracking and commodification of our locations and our personal data.[8]

The New York Civil Liberties Union (NYCLU) had warned that the LinkNYC network has significant privacy vulnerabilities, with its collection of personal information including e-mail addresses, browsing data and camera surveillance.[9] Although changes were reported to have been made to alleviate those concerns for the LinkNYC network,[10] serious doubts still remain at the NYCLU.[11] and it is not clear that any of those changes apply to the Link5G network.

At the June 7, 2023 hearing of the NYC Council Committee on Technology, the NYCLU pointed to violations of CityBridge's privacy policy found by an OTI audit, and that after nine years of LinkNYC operations, there still remains a lack of disclosure on "a detailed list of the thirty sensors included in the kiosks" and "how LinkNYC uses the personal information it collects in its ad-driven business model."[12]

Although Link5G cell towers have been touted to provide free services, including free public charging stations for cell phones, the FBI is warning against using free public charging stations as bad actors have been infecting devices with malware through these stations.[13]

Security Vulnerabilities

---

[8] CityBridge, a consortium with Google, https://www.politico.com/states/new-york/albany/story/2020/03/03/city-hall-calls-google-backed-linknyc-consortium-delinquent-1264966; CityBridge affiliated with Alphabet (Google's parent), https://www.theverge.com/2020/3/5/21166057/linknyc-wifi-free-kiosk-google-new-york-sidewalk-labs-payments-revenue. See also, NYCLU Privacy Conference which gives the history of LinkNYC and its corporate affiliations, https://livestream.com/internetsociety/hopeconf/videos/130816888.

[9] NYCLU Privacy Conference: gives the history of LinkNYC, along with privacy issues https://livestream.com/internetsociety/hopeconf/videos/130816888.

[10] https://www.nyclu.org/en/press-releases/city-strengthens-public-wi-fi-privacy-policy-after-nyclu-raises-concerns.

[11] NYCLU: "LinkNYC is a Privacy Disaster. Here's Why," July 31, 2023, https://www.nyclu.org/en/news/linknyc-privacy-disaster-heres-why; see also, https://www.techdirt.com/company/citybridge/.

[12] https://www.nyclu.org/en/publications/testimony-regarding-oversight-linknyc.

[13] https://www.theepochtimes.com/fbi-warns-against-free-public-charging-stations-for-phones-citing-hacking-risks_5184153.html?utm_source=share-btn-copylink.

Security vulnerabilities are inherent in 5G architecture and, while 5G is being deployed, these vulnerabilities have not been resolved. As to 5G's hackability, former FCC Chairman, Tom Wheeler has coined the term, the "5G Cyber Paradox," that the increased efficiency of 5G architecture renders it more insecure. "5G networks are much more vulnerable to cyberattacks than their predecessors."[14]

Whereas the 4G network is a centralized, hardware-based switching network with hardware choke points to quarantine any security breach events, 5G is a distributed, software-based network of digital routers with thousands of nodes and access points that a hacker can exploit; there is no choke point control.[15] If a hacker gains control of the 5G software managing the networks, the hacker can also control the 5G network.[16] In fact, in 2018 a hacker gained access to a Nevada casino's network through its internet connected "smart" thermostat system located in a fish tank at the casino, and was able to extract information out through the thermostat and load it into the cloud.[17] This shows that the architecture of 5G that is supposed to facilitate the Internet of Things (IoT) poses a serious risk of security breaches.

Even NYC's Chief Technology Officer and Chief Information Security Officer spotlighted 5G's security vulnerabilities in a letter to the National Telecommunications and Information Administration (NTIA) in 2020 (emphasis added):

> Such complex systems [5G] present ***more opportunities for security and privacy breaches***. By moving away from firmware-based technology of 4G telecommunication components to ***software-based***

---

[14] Why 5G Requires New Approaches to Cybersecurity, Tom Wheeler and David Simpson, Brookings Institute, Sept 3, 2019, https://www.wita.org/nextgentrade/why-5g-requires-new-approaches-to-cybersecurity/.

[15] *Why 5G Requires New Approaches to Cybersecurity*, Tom Wheeler and David Simpson, Brookings Institute, Sept 3, 2019, https://www.wita.org/nextgentrade/why-5g-requires-new-approaches-to-cybersecurity/; see also, *Why 5G Networks Are Disrupting The Cybersecurity Industry*, Oct 29, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/10/29/why-5g-networks-are-disrupting-the-cybersecurity-industry/?sh=5186fc041fe9.

[16] *Why 5G Requires New Approaches to Cybersecurity*, Tom Wheeler and David Simpson, Brookings Institute, Sept 3, 2019, https://www.wita.org/nextgentrade/why-5g-requires-new-approaches-to-cybersecurity/.

[17] https://www.casino.org/news/hackers-stole-las-vegas-casino-high-roller-database-via-its-fish-tank/;
https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/;
https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/.

> ***5G telecommunication components that will need to be updated, the opportunity for manipulation exists*** within the supply chain. Furthermore, movement away from centralized network systems to decentralized network systems ***increases the attack surface of a network***. That increased attack surface is ***amplified*** by the anticipated introduction of the increasing number and variety of connected devices (IoT) and big data industries. (top of p.3)
>
> The problem of IoT vulnerabilities will only become ***exacerbated by the increased speeds of 5G*** and other future wireless broadband technologies. (middle of p.3)
>
> IoT protection is historically poor and ***malware distribution is easily scalable***, which suggests that the creation of IoT botnets ("robot networks") for malicious purposes, including ***large-scale distributed denial of service (DdoS) attacks***, is ***likely to increase*** as well. This poses a ***significant threat*** to vital digital infrastructure and resident services at all levels of government, as well as private sector enterprise. (penultimate paragraph on p.3)[18]

To further amplify the last point, it has been reported that:

> "***Botnet and denial of service (DdoS) type attacks can bring down whole portions of the network simply by overloading a single [5G] node.***"[19]

The Mind Act (Neural Data Protection)

The Mind Act of 2025 introduced in the U.S. Senate is to protect "neural data" (brain activity, heart rate, eye tracking) from misuse, discrimination, and manipulation, and to safeguard cognitive privacy, prevent exploitation (e.g., by AI). It directs the Federal Trade Commission (FTC) to study gaps in the laws and rules for governing neural data.

---

[18] Letter from Chief Information Security Officer, Geoff Brown, and Chief Technology Officer, John Paul Farmer, to National Telecommunications Information Administration of the U.S. Chamber of Commerce, June 2, 2020, https://www.dropbox.com/scl/fi/0cxjktjxstmb825gqih25/NYC-Comments-5G-to-NTIA-6-25-20.pdf?rlkey=dgmc3m04dxd57qfz7z1g12ckh&dl=0.

[19] Why 5G Networks Are Disrupting The Cybersecurity Industry, Oct 29, 2021, Forbes, https://www.forbes.com/sites/forbestechcouncil/2021/10/29/why-5g-networks-are-disrupting-the-cybersecurity-industry/?sh=5186fc041fe9.

Conclusion

There should be no further 5G wireless deployment until privacy and security can be assured for NYC residents.

Respectfully submitted,

DocuSigned by:
Odette J. Wilkens
78664444DF89407...

Odette J. Wilkens
President & General Counsel
Wired Broadband, Inc.

Written Testimony on Int. 1335-2025
Committee on Civil and Human Rights
08 December 2025

My name is Katherine Jin, and I'm writing in support of Int. 1335-2025.

The problem
The City's current definitions of “identifying information” and “private information” were written before device-based tracking became ubiquitous. Today, device identifiers like IP addresses, MAC addresses, and mobile equipment identifiers (IMEI) function as persistent digital fingerprints. They can be used to identify, locate, and track individuals across time and contexts. Behavioral biometrics (keystroke patterns, gait analysis) are increasingly deployed to identify people, often without their knowledge.
These identifiers are routinely used to build detailed profiles of New Yorkers' movements, behaviors, and associations. But because they're not explicitly covered by City law, they fall outside existing protections.

Device identifiers are personally identifying
This isn't a contested point in the privacy community. NIST guidance recognizes that information once considered non-identifying can, when combined with other data, re-identify individuals with high accuracy. IP addresses, MAC addresses, and similar identifiers are particularly concerning because they enable persistent tracking across websites, apps, and physical locations.
The EPIC/Consumer Reports State Data Privacy Act model defines “unique persistent identifier” to explicitly include device identifiers, IP addresses, cookies, beacons, pixel tags, and mobile ad identifiers. New York State's pending privacy legislation (S.3044) similarly recognizes that devices linked to individuals warrant protection. Int. 1335 brings NYC into alignment with these frameworks.

Behavioral biometrics are an emerging frontier
The bill's inclusion of “behavioral characteristics such as keystroke and gait patterns” addresses an important gap. Unlike fingerprints or facial scans, behavioral biometrics can be collected passively and continuously, often with no notice to the individual. Keystroke dynamics are already used for continuous authentication, and gait recognition can identify individuals from surveillance footage. Both S.3044 and the EPIC model bill recognize gait as biometric information requiring protection.

Recommendation
The Council should pass Int. 1335-2025. This is a straightforward definitional update that ensures City privacy protections keep pace with how tracking actually works now. Without it, New Yorkers remain exposed to identification methods that existing law wasn't designed to address.

Thank you for the opportunity to submit testimony.

Katherine Jin

Lead For Humanity

Michele Anne Blondmonville

Contact

[redacted]
Cambria Heights, New York
11411
[redacted]
Lead4humanity6@gmail.com

New York City Council
City Hall
250 Broadway
New York, New York

Dear Elected Officials,

My name is Michele Anne Blondmonville. I am a Health and Fitness Educator for 40 years: a former Adjunct Lecturer at New York University, former Instructor at Fashion Institute of Technology, Trainer at The American Red Cross, American Heart Association, and other health facilities in the State of New York.

Thank you for your servitude in these difficult times. I am speaking on behalf of everyday people who are Havana Syndrome or Anomalous Health Incident Victims- some knowingly and others unknowingly. With the glaring awareness of the benefits afforded to our diplomat counterparts: Helping American Victims Affected by Neurological Attacks (HAVANA) Act of 2021 (Public Law 117-46) we certainly hold fast to the notion that one day we will be free from torture, pain, invisibility, and the weaponization of technology. Havana Syndrome includes remote access to the biology of a human being.

Everyday People Havana Syndrome Victims (EPHSV) is comprised of diagnosed Havana Syndrome public citizens who have been unlawfully experimented on and who endure targeting in various nefarious manners. These heinous crimes include but are not limited to organized stalking, smear campaigns, noise harassment , electronic assault from directed energy weapons, non consensual, human experimentation- socially and technological such as voice to skull (V2K), blue eye technology, and AI. They are put on illegal lists unknowingly that are distributed to various agencies for this experimentation for vindictive reasons, technological research and political harassment (whistleblowers, activists, etc). Noone should have their brain interfaced to a computer or AI Program. We are assaulted 24 hours a day randomly for compliance and are remote neuromonitored.
We would like New York to adopt laws that protect our neural data and like California Laws SB1223 and Colorado House Bill 24-1058 protecting brain data collected by devices and also Repeal the

Lead For Humanity

Beverly Blondmonville

Contact

Bbbev42@gmail.com

New York City Council
City Hall
250 Broadway
New York, New York

Dear Elected Officials,

My name is Beverly Blondmonville. I have worked at Chase Manhattan Bank for most of my life- my 20's until retirement as an IT (Technology Analyst). I worked on Y2K ATM's making sure the technology was in compliance for our entry into the year 2000 (our 21st Century) Fast Forward to my retirement – experimented on with various technologies. It hurts I am tortured 24 hours randomly 7 days a week at the mercy of whoever has access to my biometrics I am asking for advocacy and support to protect my rights.

Thank you for your consideration Beverly Blondmonville

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: December 8 2025

(PLEASE PRINT)

Name: Michele Blond monville

Address: [redacted] 220th Street

I represent: _____

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☑ in favor ☐ in opposition

Date: 12-8-25

(PLEASE PRINT)

Name: Beverly Blondmonville

Address: [redacted]

I represent: _____

Address: Jamaica Hts NY 11411-1161

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Susan Peters

Address: [redacted]

I represent: New Yorkers for Wired Tech

Address: _____

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Clayton Banks

Address: [redacted] Frederick Douglass Blvd

I represent: Harlem

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Richie Lipkowitz

Address: [redacted]

I represent: self

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: 12/8/25

(PLEASE PRINT)

Name: ALEX SPYROPOULOS

Address: _____

I represent: TECH:NYC

Address: _____

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1335, ~~Res. No. 708~~ Res. No. 783

☒ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Talia Kamran

Address: 177 Livingston St., Brooklyn, NY

I represent: Brooklyn Defender Service

Address:

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Michael Fitzpatrick

Address: Chief Privacy Officer

I represent: City of NY

Address: (Brooklyn-ZMTC)

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: 12/08/25

(PLEASE PRINT)

Name: Alissa Johnson

Address:

I represent: Surveillance Technology Oversight Project

Address: 40 Rector St

Please complete this card and return to the Sergeant-at-Arms