



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 2017), <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 initiative⁷, through programs like Worker Connect in 2010⁸, LinkNYC in 2016⁹, Big Apple Connect in 2022¹⁰ and continuing past the launch of MyCity in 2023¹¹, 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 Controversial 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/NYCAadmin/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.