TESTIMONY OF MINDY TARLOW, DIRECTOR
MAYOR'S OFFICE OF OPERATIONS

BEFORE THE
NEW YORK CITY COUNCIL

COMMITTEE ON TECHNOLOGY

FEBRUARY 1, 2016

Good afternoon Chairman Vacca, and Members of the Committee on Technology. My name is Mindy Tarlow, and I am the Director of the Mayor's Office of Operations ("Operations"). I am here today with two colleagues from Operations: Laura Negrón, Chief Privacy Officer and Special Counsel, and Tayyab Walker, Director of Enterprise Data Solutions. On behalf of the Administration and my colleagues, I would like to thank you for the opportunity to testify at this hearing.

INT 627 proposes new and broad-sweeping requirements governing personal information privacy and security. We understand that this legislation is motivated by the laudable goals of preventing unlawful public access to residents' sensitive personal information, and ensuring diligent data stewardship and security by entities and persons having such information in their custody. This is a position we wholeheartedly support.

Although the Administration unequivocally believes in the importance of personal privacy and data security, and the need for robust protocols and practices to safeguard individuals' personal data,

we are concerned that this legislation will inadvertently impede the delivery of critically needed services to New Yorkers and the human services research currently made possible through legally authorized inter-agency data exchanges that are facilitated through technology.

As written, INT 627 would restrict City agencies from collecting, using, and sharing clients' personal information, except for those purposes relevant to an agency's mission. With few exceptions, this legislation requires clients' prior written consent for disclosure of their personal data outside of the agency that collected it, and requires agencies to notify clients of any and all intended uses. These provisions will not only constrain unfettered public disclosure, which we understand and agree is critical, but unfortunately, in practice, these provisions will equally apply to the kinds of confidential inter-agency data exchanges that are needed to deliver coordinated client services, and conduct valuable research studies.

While complying with privacy laws, the City must also fulfill its duty to responsibly serve its children, adults, and families, and break

down information silos between agencies that impede effective and timely service delivery. As you know, New York City's agencies deliver a vast array of services each year to millions of people, many of whom are served by multiple agencies. Each agency is separately tasked with identifying client needs, determining eligibility, delivering services, providing case management, and evaluating client outcomes. Coordination of services among and between City agencies is challenging but essential to providing the right services to clients at the right time, and in many instances is critical to averting an impending health or safety crisis.

In the past decade, the City has developed a number of citywide programs and initiatives facilitated by technology innovations that have made coordinated service delivery increasingly possible. For example, through algorithm-based data-matching, knowledge held by one agency that a child's family was at risk of eviction for non-payment of rent enabled a City worker from a different agency to help the family secure public benefits and avoid homelessness. Also through

interagency data exchange, the City has been able to conduct comprehensive outreach to families of children eligible for Pre-K, and enroll tens of thousands of children. We have located families of toddlers abandoned in Port Authority, identified safe havens for victims of suspected abuse, and prevented vulnerable elderly people from eviction.

We already have robust, legal privacy compliant processes and data stewardship protocols in place governing our technology facilitated data-sharing initiatives, which we would like to explain here. When an agency identifies a need for another agency's client data, the requesting agency prepares a business use case that is vetted by both Operations' Chief Privacy Officer and counsel for the agency data owner(s). The use case must describe, in writing, the specific data elements needed, users who will have access to the information, and the purpose for which the information will be used. Each data element is separately analyzed to determine whether it may legally be disclosed for the purpose proposed, and only those data elements authorized by

law for sharing are approved. In accordance with City IT security policy and applicable law, any confidential client data approved for sharing is transmitted — and must be stored — in encrypted form. Overarching legal agreements, signed by participating parties, memorialize agencies' obligations to comply with strict data use, access, confidentiality, and data security protocols.

We believe that INT 627, while raising important concerns, is over-broad, and as a result, could unintentionally have a chilling effect upon the City's continued ability to coordinate these critically important inter-agency data exchanges for the limited purposes of providing clients with benefits, services and care, and ensuring their safety. We are concerned that the bill's provisions may unravel the good progress that we have made toward achieving the "one-city" vision of client services for New Yorkers articulated by this Administration.

There are certain provisions in the proposed legislation that are of particular concern. These restrict the collection and maintenance of

information about an individual only as needed to accomplish an agency purpose required or authorized by law. We believe that these provisions could undermine agencies' ability to collect and maintain client information from *other* agencies for future integrated service delivery purposes where the same client is served by multiple agencies, many of which may not be known at the time of initial data collection by an agency.

The extensive notice provisions in the legislation concerning the use of an individual's data not only present significant operational challenges for agencies serving a large volume of clients, but could also undermine the City's ability to rely on existing legal privacy exceptions that permit the exchange of data between agencies without such notice requirements — particularly in emergency circumstances, such as finding a relative to house a child in cases of suspected abuse or neglect, and under similar circumstances where notice is not feasible.

INT 627 requires client consent to disclose personal information outside of the agency that collected it, with very few exceptions. These

include disclosure for certain law enforcement purposes, in response to court orders, and where specifically authorized by state or federal law or regulation. These enumerated exceptions overlook local laws that permit interagency data-sharing without client consent to provide benefits, services, and care. There are also federal and state legal exceptions permitting disclosure of confidential client information that do not contain data collection restriction and notice requirements. It is unclear how those imposed by this legislation would be reconciled with federal and state legal exceptions that do not contain them.

We note for your consideration that INT 627's consent requirements do not address instances where an individual may lack the capacity to consent due to mental health issues, age (in the case of minors), or other circumstances, leaving the provision open to further legal interpretation and debate.

We also want to point out that the consent restrictions could inadvertently restrict the important work of Municipal Archives, which

provides invaluable historical documents to the public containing exactly the type of information prohibited from disclosure.

Finally, we are concerned that the proposed legislation imposes new requirements for records retention and data destruction that may create ambiguity in the City's records management processes, and could have the additional unintended consequence of impairing important research that relies on the availability of historical client data.

To conclude, we believe that the important privacy and data security protections sought by this legislation are already embedded in existing, robust City practices and protocols. We are concerned that, despite its well-meaning intentions, this legislation, as written, would inadvertently impede the City's ability to deliver coordinated services to New Yorkers, create ambiguity through its terms, and cause confusion in relation to existing privacy and other laws. If enacted, this could not only set back the City's progress in data analysis, integrated case management, and human services research, but we believe it might

also discourage future technological innovations that could further improve the delivery of City services to our children, adults, and families.

The City has raised its concerns about INT 627 with the bill sponsor, who has been receptive to further discussion on the issues. We also wish to reiterate that we are aligned with what we believe is the underlying goal of INT 627: to ensure that our City has sufficiently rigorous protections in place to safeguard the privacy of personal data. We look forward to our continued conversations concerning this legislation. Thank you and we are happy to answer any questions you may have.

DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS TESTIMONY
BEFORE THE NEW YORK CITY COUNCIL COMMITTEE ON TECHNOLOGY
RE: INTRO. 626-2015 / PERSONAL INFORMATION SECURITY &
INTRO. 1052-2016 / CITY AGENCY ELECTRONICS DISPOSAL
MONDAY, FEBRUARY 1, 2016

Good afternoon Chair Vacca and members of the Council Committee on Technology. My name is Anne Roest, New York City Chief Information Officer and Commissioner of the Department of Information Technology and Telecommunications, or DoITT. Thank you for the opportunity to testify today on Intro. 626, in relation to the security of personal information; and Intro. 1052, in relation to the disposal of electronics for City agencies. Taken together, these bills aim at addressing a constant imperative of the digital world – information security – and I thank the Committee for its focus on such a vital area of City operations. I am joined today by Mindy Tarlow, Director of the Mayor's Office of Operations, who will speak to Intro. 627.

In a connected city our IT security posture is only as good as the weakest link, and a weak link successfully exploited in one agency can have significant consequences on other agencies – and on the lives of the New Yorkers they serve. Accordingly, DoITT maintains and promulgates a range of Citywide Information Security Policies and Standards as strong and dynamic as the city we serve, to which every agency must adhere.

Our robust IT Security Division also manages the overall security of the City's shared data and information technology assets through the management of an integrated security network, consolidating desktop and server security on a single, citywide platform. DoITT also maintains email, intrusion prevention systems, next generation firewall protection, and security monitoring. In this way, New York City maintains the ability to keep pace with rapidly-evolving threats by centrally implementing and enforcing citywide policies and standards – with the ability to update them dynamically.

There is always the opportunity to further improve upon the job we do – and in an area as vital as IT security, it is essential to do so. New York City is an incredibly inviting target for our cyber adversaries the world over, and these parties are constantly developing new and increasingly complex means of attack. The City, in turn, must have the ability to keep pace with these rapidly-evolving threats by centrally implementing and enforcing citywide policies and standards, and by continuing to update them as necessary.

To that end, the de Blasio Administration has been aggressive and progressive in its support of a strong cyber security program. Since the start of the Administration we have increased our security headcount and invested tens of millions of additional dollars in new training and technologies to improve our security posture and to keep pace with the ever-evolving threat landscape.

Together these measures reflect the great emphasis we place on protecting the security of New Yorkers' information against the many thousands of daily attempts to improperly access City systems and data. The spirit and aim of **Intro. 626** align with these efforts, and with the high standards New Yorkers expect and deserve when entrusting the City with their personal information. I very much appreciated the opportunity to discuss with the Council last week my concerns on the bill as drafted, and look forward to continuing our dialogue about the City's cyber security program. Our interest, and the Council's, in protecting sensitive information could not be more closely aligned.

Next, **Intro. 1052**, would require City agencies to ensure erasure of all information when disposing of electronics. The City recognizes the importance of such a practice, and our Citywide Information Security Policy on Digital Media Re-use and Disposal, established in 2011, requires that all digital media undergo a data sanitization process prior to disposal, or reuse, to protect against unauthorized access to information. Not only is this a policy to which all City employees must adhere, but it is also one that any vendor handling any of our equipment must adhere to as well. We will continue updating this policy as new electronic tools become available, and are happy to keep the Council apprised of our progress.

I appreciate the opportunity to testify today. And I thank the Council for highlighting the vital issue of information security. By developing policies nimble enough to adapt to the ever-evolving and sophisticated means of technological attack, within a centralized framework of current best practices, we can continue successfully protecting the information of New Yorkers.

I look forward to working with you.

Thank you.

Digital Media Re-use and Disposal Policy

The Policy

All digital media must undergo a data sanitization process prior to disposal or reuse to protect against unauthorized access to information.

Data Sanitization Procedures will be internally documented by each agency.

Scope

All digital media, file systems and non-volatile storage devices including but not limited to desktop and laptop computers, servers, photocopiers, fax machines, portable and internal hard drives, optical media (e.g., CDs and DVDs), magnetic media (e.g., tapes, diskettes), non-volatile electronic media (e.g., memory sticks), portable devices, cell phones and smart phones are covered under the provisions of this policy. All such devices are referred to collectively as "digital media" in this policy.

Approved Methods for Data Destruction

Where any equipment containing digital media is to be discarded or re-used, donated, sold or otherwise transferred to an external person, organization or vendor (e.g. at the end of a lease or as an RMA (returned merchandise), the City agency must use one of the following approved methods appropriate for rendering all information on the media permanently unreadable:

a. A data wiping program which will securely delete all data by methods that irreversibly wipe the physical area of storage (rather than simply removing the disk-directory reference to that information).

b. Any full disk encryption method which is compliant with the Citywide Encryption Policy and in which it can be reasonably expected that no unauthorized person has the ability to decrypt the data.

c. Degaussing and/or physical media shredding technology which meets NIST standard 800-88 (or its successor):

   http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

Agency support staff may evaluate data stored on any equipment transferred *internally* (within the agency or between City agencies) and bypass the requirements of this policy. All such cases must be documented and approved by agency management to ensure accountability.

An asset can be transferred for disposal to a vendor who has contractually committed to following one or more of the above methods.

Document Revision History

Date	Description
May 20, 2011	**Version 1.0** published.
June 16, 2011	**Version 1.1** Updated header with new NYC logo and added this revision history table to the document.
Sept. 9, 2014	**Version 1.2** Policy review and minor formatting updates.

OFFICE OF THE PRESIDENT
BOROUGH OF MANHATTAN
THE CITY OF NEW YORK

1 Centre Street, 19th floor, New York, NY 10007
(212) 669-8300 p (212) 669-4306 f
163 West 125th Street, 5th floor, New York, NY 10027
(212) 531-1609 p (212) 531-4615 f
www.manhattanbp.nyc.gov

Gale A. Brewer, Borough President

Gale A. Brewer, Manhattan Borough President
Testimony for New York City Council Committee on Technology
Intro 626 & Intro 627
February 1, 2016

My name is Gale Brewer and I am the Manhattan Borough President. I want to thank Committee Chair James Vacca for holding this hearing today, as well as the staff for their hard work. I am here to speak about two bills that have been introduced at my request by Council Member Ben Kallos, Intro 626 and Intro 627. The legislation would require each city agency to develop comprehensive security protocols to ensure that personal information of all city residents who interact with an agency be protected. I first introduced this legislation several years ago when data breaches in city agencies became evident. Perhaps the most famous was the 2010 theft of 1.7 million HHC medical records from a van. The widespread use of technology brings benefits, but also growing risks of hacking, identify theft, and other cyber-crime related challenges. As a city, we must ensure that personal information we collect is protected using the most up-to-date methods.

At the initial hearing on this legislation in 2012, the Department of Information Technology and Telecommunications (DoITT) expressed support for the spirit of data security legislation, but had concerns about specific bill language. To their credit, the staff at DoITT have promulgated a citywide IT security policy, including requirements for contractors and vendors that personal information, including that stored on removal media, be encrypted. I hope that today's hearing will update us on the current status of DoITT's policies, and start a new conversation on how best to protect client data in New York. Much has changed since that 2012 hearing, notably the passage of another bill I sponsored, New York City's Open Data Law. The Law requires that agencies publish data to a single portal in machine-readable formats, while removing any personally identifiable information that could cause security concerns. These dual requirements to publish data, while protecting the release of anything that could be used to harm an individual's privacy, are at odds with one another, but surely not insurmountable. I expect that changes must be made to Intros 626 and 627 to ensure full compatibility with the letter and spirit of the Open Data Law, while protecting the privacy and security of all New Yorkers.

For example, there is a list of exceptions in the current draft of the legislation which would allow disclosure of personal information where required by federal or state laws. It may make sense, as was suggested to me by some advocates, to include additional exceptions in order that specific data can continue to be disclosed in compliance with the spirit and intent of the Open Data Law. This would allow agencies to continue publishing information, such as

addresses of those with open construction permits, which might become restricted under an unreasonably strict interpretation of "personal information" envisioned by Intros 626 and 627. It is certainly not my intention to pass any legislation that would threaten the city's open data program, which I have spent years working to develop. The default setting for non-personal information must remain open.

However, I also think it is crucial for the future of the city's open data program, as well as the international open data movement, to send a clear signal that personal information security and open data are not mutually exclusive. For personally identifiable information such as Social Security Numbers, private health information, etc., data security across all agencies must be maintained. We have begun conversations with the Administration on some potential amendments to the legislation to protect DoITT's ability to promulgate additional protections on top of the minimum standards established by this legislation. It is certainly not my intention to prohibit the Administration from keeping pace with advances in technology, nor to proscribe specific technology that may become irrelevant in a short time period. Rather, the intent of this legislation is to establish a baseline in law that all agencies must comply with.

I look forward to working with the Council and the Administration to find a compromise that protects the privacy and security of personal data, while expanding on the successes of the City's open data program. Thank you again for inviting me to testify, and I am happy to answer any questions you may have.

To: NYC Council - Committee on Technology
From: Noel Hidalgo, Executive Director of BetaNYC

Re: **Int 0626-2015 & Int 0627-2015**

1 February 2016

To the NYC Committee on Technology & Chairperson Vacca,

Through the support of this committee, New York City's civic technology and open data community is larger than ever. Today we are 3,200 member strong. This year, our numbers will grow to include many more Community Board members. In partnership with the Manhattan Borough President Gale A. Brewer, we have launched a Civic Innovation Fellows program. We are partnering CUNY undergraduate students with Manhattan Community Boards with the goal of marrying technology, data, and design to increase hyper-local civic participation.

The Civic Innovation Fellows program is a part of my research fellowship at Data & Society Research Institution. Located in Manhattan's Flatiron District, our research is focused on social, cultural, and ethical issues arising from data-centric technological development.

Significant ideological and technological concerns have come up with Int 0626-2015 and Int 0627-2015.

Int 0626-2015 – Personal information security.

In an age when the Federal, State, and Municipal governments are demonizing cryptology, aka math, we are very happy to see our City Council outline a citywide policy embracing cryptology and a universal desire to secure information.

As you know, Council offices and Community Boards are on the front lines of solving problems. Historically, they are under resourced. When it comes to using technology to catalog and address community issues, we are not sure this bill takes their constraints into consideration. Volunteers have a unique role within New York City government and this bill seems to ignore them.

If enacted as written, we see a negative impact on how Council Members and Community Boards use, send, and receive information. If enacted, we foresee an increased burden on Council and Community Boards offices. This bill scatters many more locks and keys the City's

technology infrastructure. From my professional experience, these burdens are best addressed with dedicated staff, increased training, and modernization of technology.

BetaNYC and Data & Society are available as resources to convene stakeholders and ensure constituent services, civic volunteers, and distributed, secure 21st century government information systems are properly balanced.

Int 0627-2015 — Securing personal information privacy.

This bill contains our community's greatest concern. As our peers from the NYC Transparency Working Group will testify, personal information is attached to many open data sets. The data this bill is trying to exclude might remove our ability to look at permits, property records, financial records, campaign contributions, and public safety records.

BetaNYC is here to warn the Council that the bill's current language might prevent Council Members, Community Boards, and members of BetaNYC community from doing their jobs.

Since this bill was introduced, I have received several concerns from businesses, city employees, and the City's non-profit service providers. This bill potentially harms the City's open data achievements, it would place undue constraints to the City's service providers, advocacy organizations, public interest organizations, journalists, and everyday New Yorkers who need access to public records.

This bill seems to protect public information at the cost of public interest. BetaNYC and Data & Society are willing to be resources and help the Council convene stakeholders to make sure that government information systems strike the right balance between privacy and public interest.

Summary

We are extremely fortunate to have a City Council that understands the nuance of protecting privacy and supporting public interest. We are thankful that this City Council is forward thinking and willing to discuss things others fear. We look forward to further conversations to weigh these bills' appropriateness. Thank you.

February 1, 2016

Reinvent Albany

Testimony of

Dominic Mauro, Staff Attorney, Reinvent Albany

before the

New York City Council Committee on Technology

Hearing on Personal Information Security on February 1, 2016

Good afternoon Chairman Vacca and Members of the Technology Committee, I am Dominic Mauro, Staff Attorney of Reinvent Albany, a good government watchdog which co-chairs the New York City Transparency Working Group. I am also presenting this testimony on behalf of my Transparency Working Group Co-Chair and NYPIRG Senior Attorney, Gene Russianoff, who was unable to attend today.

We are concerned that overly broad language in Intro 626-2015 and 627-2015 may undermine the assumption that city data is "open by default" under the Open Data Law. We believe these bills could force numerous data sets on the open data portal to be taken offline or redacted. While we understand that the intent of these bills is to protect New Yorkers' personal information, we ask the NYC Council to delay further legislative action on Intro 626 or 627 until Corporation Counsel provides an opinion on what implications these bills have for the implementation of the city's Open Data Law and other data the city has already published online.

Both bills regulate the publication of Personal Information, which is defined as "any information concerning an individual which, because of a name, number, symbol, mark or other identifer, can be used to identify that individual." is is an extremely broad definition which may cover many data sets on the open data portal; there may be hundreds which contain information that "can" be used to identify individuals. For example, ACRIS, OATH's Environmental Control Board hearings, DOB Job Permits, and the Campaign Finance Board's dataset of Political Contributions.

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 627 Res. No. _____

☐ in favor ☐ in opposition

Date: 2/1/16

(PLEASE PRINT)

Name: TAYYAB WALKER

Address: TITLE: DIR. PRODUCT DATA SOLUTIONS - G

I represent: NYC OPERATIONS

Address:

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 627 Res. No. _____

☐ in favor ☐ in opposition

Date: 2/1/16

(PLEASE PRINT)

Name: MATTHEW KLEIN

Address: SPECIAL ADVISOR FOR SERVICE INNOVATION

I represent: NYC OPERATIONS

Address:

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 627 Res. No. _____

☐ in favor ☐ in opposition

Date: 2/1/16

(PLEASE PRINT)

Name: MINDY TARLOW

Address:

I represent: DIRECTOR OF THE MAYOR'S OFFICE OF OPERATIONS ("OPERATIONS")

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. 626/627 Res. No. _____

☐ in favor ☒ in opposition

Date: 1FEB2016

(PLEASE PRINT)

Name: NOEL HIDALGO

Address: BROOKLYN, NY

I represent: BETA 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. 626/627 Res. No. _____

☐ in favor ☐ in opposition

Date: 2/1/16

(PLEASE PRINT)

Name: Will Colegrove

Address: 1 Centre St

I represent: Manhattan Boro Pres

Address: 1 Centre St

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. 626/1052 Res. No. _____

☐ in favor ☐ in opposition

Date: 2/1/16

(PLEASE PRINT)

Name: ANNE ROEST

Address: _____

I represent: CHIEF INFORMATION OFFICER AND COMMISSIONER

Address: OF THE DEPT. OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS (DOITT)

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: Dominic Mauro

Address: _____

I represent: Reinvent Albany

Address: _____

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