DEPARTMENT OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS TESTIMONY BEFORE THE NEW YORK CITY COUNCIL COMMITTEE ON TECHNOLOGY

Oversight: Privacy of City Data

Monday, April 24, 2017

Good afternoon Chair Vacca and the members of the NYC Council Committee on Technology. My name is Anne Roest, and I am the City's Chief Information Officer and Commissioner of the Department of Information Technology and Telecommunications (DoITT). I am joined by Mindy Tarlow, the Director of the Mayor's Office of Operations and Chief Technology Officer (CTO) Miguel Gamiño, in addition to two of my DoITT colleagues, Michael Pastor, DoITT's General Counsel, and Geoffrey Brown, the Citywide Chief Information Security Officer (CISO). Thank you for the opportunity today to testify on the privacy of City data. I commend the Committee for its timely examination of this topic.

I want to begin by articulating the values that animate our work at DoITT, and across the entire administration, with respect to data privacy. I believe, as do my colleagues beside me, that New Yorkers' private information should stay that way—private. We also believe that the City's systems and assets must stay secure, shielded from outside threats. This is what drives our work every day.

I know that the Council shares these values, and we are grateful for your collaboration on these critical fronts, particularly in a time when the actions of the federal government appear to be working against the privacy and security of New Yorkers.

I'd first like to highlight DoITT's work in this arena by focusing on our excellent Citywide Cybersecurity team, which leads the effort to protect the City's systems and assets from ever-evolving cyber threats. This administration has made a tremendous commitment to fortify the cybersecurity team in recent years, with a significant increase in investment for enhanced technology to stay ahead of these threats, and the addition of a Citywide CISO to spearhead proactive and progressive risk-management strategies. That has put the City in a better position than we've ever been on that front.

One strategy the cyber team has employed is intensifying the role of employees in the defense of our networks. We recently created a security awareness video to help employees understand the importance of using strong passwords—a simple but extremely effective way to protect our systems. We have subsequent videos in development, including one scheduled for release in May.

A second strategy recognizes phishing as a significant attack vector. Phishing is the use of emails to trick a victim into clicking a malicious link or into providing sensitive data. We've started launching test phishing emails—a standard security practice—to see how employees respond, and subsequently perform detailed analysis and provide training for those who need it. At the same time, we are strengthening the technical defenses to our Citywide email flow.

The Cybersecurity team also establishes Citywide Information Security policies and standards, to which city agencies and their employees must adhere. These policies and standards, which we are currently updating, inform the practices of all City agencies' interactions with the public—both online and in person.

People are thinking about privacy now more than ever. With that in mind, I can detail a few more forward-thinking policies that keep New Yorkers' information secure.

Data Classification and Encryption

We are very proud of our laws and policies that promote transparency. However, much of the information collected, generated, or maintained by the City is not public record and should remain as such—including the personal information that New Yorkers provide to agencies. To that end, one of DoITT's most vital information security policies is the data classification policy, which ensures that agencies 1) appropriately categorize their information assets, and 2) apply the appropriate degree of protection to that information. This is critical because all data with a classification of "private" or "confidential" may not be stored and/or transmitted across any communication mechanism unless it is protected using approved encryption technology.

Security Assurance

Similarly, applications – whether public-facing or internally accessible – must go through a software security assurance process. This ensures that the tools that the City develops to support City functions are built in a secure fashion, and must comply with our robust policies, standards, and industry best practices. For example, the Department of Finance just released a new mobile application to either pay or dispute a parking ticket. As anyone who has had to go through that process knows, it may be necessary to enter credit card information, which must be transmitted over a secure network. The security assurance process gives New Yorkers confidence that this convenience does not require a trade-off for safety.

Electronics Disposal and Digital Media Re-Use

The proper physical storage of data, and destruction of that data when the physical vessel is no longer in use, is extremely important. That is why DoITT formulated a digital media re-use and disposal policy, requiring that all digital media—such as computers, flash drives, smartphones, or photocopiers—undergo proper data sanitization when the devices will no longer be used. With this committee's guidance, a new law has been passed to codify this policy. Taken together, the law and policy ensure that any private information that agencies store could never accidentally fall into the wrong hands.

LinkNYC Privacy Policy

These and our other Citywide information security policies are thorough and effective for City agencies, but DoITT's role in data privacy does not end there. Wherever possible, we leverage our franchises to better educate New Yorkers of their rights, while enhancing privacy protections.

Over 1.4 million residents and visitors have connected to LinkNYC, the City's first-of-its kind franchise to transform outdated payphones into state-of-the art free Wi-Fi kiosks. This is one of the few franchises that this administration negotiated from beginning to end, and it was our priority from the start to negotiate a strong, user-first privacy policy with our franchisee, CityBridge.

Just a month ago, we unveiled an update to the privacy policy that made clear that CityBridge does not, and will never, store browsing history, track the websites that Wi-Fi users visit, or share or sell data to third parties. This latest version of the privacy policy was applauded by the New York Civil Liberties Union (NYCLU) for being responsive to concerns and improving privacy protections for LinkNYC Wi-Fi users, and we are unaware of a public Wi-Fi network that has a stronger privacy policy.

The LinkNYC privacy policy, taken together with the privacy policy for Queensbridge Connected, to which the CTO will soon speak, demonstrates that the City has set the bar high for privacy considerations across the board. We look forward to continuing the discussion with this committee today.

Federal Actions

Before concluding, I'd once again like to reinforce that we share the Council's concerns about recent actions on the federal level. As you know, Congress recently passed, and the President signed, legislation that unravels essential protections of Americans' online privacy. Unfortunately, with the leadership in place in the White House, Congress, and the Federal Communications Commission (FCC), these kinds of mandates will only become more commonplace. We will continue to monitor these efforts and comment as necessary in collaboration with the CTO's office, but we also welcome your feedback and suggestions on these crucial matters.

Data privacy is an urgent consideration that the City takes very seriously. I hope my testimony has underscored that. Thank you for the opportunity to testify today, and I will now turn it over to Miguel Gamiño, the City's Chief Technology Officer, to provide more detail on broadband privacy and Internet of Things.

###