NYC
Mayor's Office of
Information Privacy

November 22, 2019

Testimony of Laura Negrón, Chief Privacy Officer of New York City

Before a joint hearing of the New York State Senate Standing Committee on Consumer Protection and Standing Committee on Internet and Technology:
"Protecting Consumer Data and Privacy on Online Platforms"

Mayor's Office of
Information Privacy

Introduction
Thank you to Chair Thomas, Chair Savino, and the members of the Standing Committees on Consumer Protection and Internet and Technology. My name is Laura Negrón, the City's Chief Privacy Officer, head of the Mayor's Office of Information Privacy, and General Counsel to the Mayor's Office of Operations.

Together with the City's Chief Technology Officer, the New York City Department of Information Technology and Telecommunications, and the New York City Cyber Command, I submitted testimony at the last hearing your Committees held on privacy matters earlier this year. We appreciate the opportunity to discuss the City's experience and expertise on this important issue, and to partner with your Committees on legislative measures that help strengthen legal privacy protections for New Yorkers.

The City's role in protecting residents' privacy interests
The City of New York has a comprehensive privacy protection framework in place. In 2018, the Mayor named me as Chief Privacy Officer. In this role, I am tasked with protecting the identifying information of New Yorkers in their interactions with City government, and leading the Administration's broader policy and advocacy work on privacy protection. I am joined by the Mayor's Office of the Chief Technology Officer as well the Department of Information Technology and Telecommunications.

Our offices together represent a citywide commitment to privacy and confidentiality protections and promoting public trust in accessing both municipal and non-governmental services and resources. In this era of rapid growth in complex—and increasingly digital—data collection and data sharing, our work is crucial to protecting the rights and interests of New Yorkers.

Protecting people's privacy online
Safeguarding the privacy of individuals' personal information that has been entrusted to government is essential to delivering services, such as health care, education, public safety, cash assistance, and more. As an increasing number of public and private services provide online access, or even require it, the need for consumer privacy protection online has grown exponentially.

Legal privacy protections have not always kept up with advances in technology, and that is the case now in consumer activity online. Web-based transactions may involve the collection of a wide range of personally identifying information, which in many cases is retained, analyzed, shared or sold with other parties without the consent or understanding of users. As we have seen time and time again in recent years, these practices have both fueled the growth of many innovative businesses and technologies, while at the same time have resulted in harmful data breaches and blows to the confidence of consumers who had thought their information was being appropriately handled.

One such practice that in particular merits further consideration as a policy and legislative matter is the issue of the disclosure and sale of consumers' information to companies functioning as

"data brokers." These companies collect, compile, and process immense volumes of data about individuals with whom they may not have a direct relationship and subsequently sell elements of that information to other companies that may seek to use it for targeted advertising, credit reporting, voter targeting, or other purposes. Given the concerns about consumer consent and awareness of these uses of their personal information, it is important to consider how to address the risks that this type of practice raise, and to understand the experiences of other states that have legislated in this area. We look forward to continuing conversations with the Committee members about this issue.

Importantly, we must also keep in mind that practices which diminish consumer confidence in businesses can also diminish their confidence in the public sector to protect their privacy. This diminished confidence could potentially discourage people from reaching out to government agencies that provide vital services they need. So, in addition to the role that government must play in consumer protection, the City has also recognized the imperative of ensuring residents can interact safely and appropriately with government agencies that provide public assistance benefits, health care, policing, and other critical services.

The New York Privacy Act (S5642/A8526)

We are encouraged that the Senate and Assembly are considering the New York Privacy Act. The bill offers great promise in establishing valuable legal protections and rights for consumers, building upon the foundation of the kinds of privacy laws and policies regulating government interactions in New York City and beyond.

The bill contains a number of provisions that would be very valuable in protecting New Yorkers' privacy in commercial interactions, both online and offline.

We support the flexibility incorporated into the definition of "personal data," which is presented as a nonexclusive list, recognizing the need to be responsive to future technology developments.

We support the idea that businesses must exercise a fiduciary duty to consumers with regard to their personal data.

We also support the clear definition of consumers' rights related to their personal data, such as the requirement of an opt-in process to businesses' use of personal data, including third-party data-sharing and sale; the right to demand an accounting of personal data collections and disclosures, the right to receive a copy of personal data maintained about them; and the rights to correct inaccurate information and request deletion of personal data in certain circumstances.

These are crucial measures and would help ensure that consumers have real control over the uses of their own information.

We are also supportive of the bill's recognition of the distinctions between commercial enterprises' collection and use of personally identifying information, as opposed to government agencies' (and our contractors') collection and use of such information for purposes such as the

administration of public benefits and services or for research. The City of New York has developed a comprehensive set of standards and guidelines for the protection of identifying information by the local government, and the bill appropriately ensures that this protective structure would remain in place.

Conclusion

Thank you very much to the Chairs and the members of the Committees. We are grateful that this issue is being prioritized by members of the Senate and we look forward to continuing conversations on the New York Privacy Act and other privacy and technology matters in the future.

Mayor's Office of the
Chief Technology Officer

TESTIMONY
Presented to the
New York State Senate Standing Committee on Internet and Technology and
New York State Senate Standing Committee on Consumer Protection
on the subject of Protecting Consumer Data and Privacy on Online Platforms
on Friday, November 22, 2019

Chair Savino and Chair Thomas, my colleagues and I appreciate the opportunity to testify today on the important topic of protecting consumer data and privacy online. My name is John Paul Farmer and I serve as the Chief Technology Officer (CTO) of the City of New York.

The Mayor's Office of the CTO addresses high-priority gaps for which privacy guidelines and standards are needed to increase the digital privacy protections for consumers outside of their interactions with local government. The office's work on digital privacy includes research, programming, stakeholder engagement, and development of legislation, policies, and standards regarding core and emerging technologies.

The issue before us today is one of paramount importance for the state to grapple with as technology increasingly becomes the gateway for New Yorkers' participation in our professional, educational, civic, and social communities. My colleagues and I appreciate that the legislature is proactively developing a comprehensive approach to protecting the digital privacy of New Yorkers. The U.S. Congress's repeal of the Federal Communications Commission's (FCC) 2016 internet service privacy protections makes action by the State and City essential. Our three offices submitted written testimony for your June 2019 hearing on online privacy and are pleased to share further considerations as you continue to develop the Senate's approach.

New York City's Approach to Digital Rights and Privacy
New York City recognizes that privacy is a critical issue in the digital age for all residents, and is an even greater threat to vulnerable New Yorkers. Based on national research, online privacy concerns disproportionately impact low-income people, those who are foreign born, and seniors. Black and Hispanic adults indicate higher levels of concern about not knowing what personal information is being collected about them or how it is being used. Women also have greater concerns than men about online privacy, and as a group, and face particular threats to their digital privacy.

To address these disparities and concerns, starting early in Mayor de Blasio's administration, the City developed a multi-faceted approach to building an inclusive digital society: defining foundational

principles, leading a coalition of allied cities, developing digital inclusion resources, engaging businesses in developing tools, and establishing policies and legislation.

The foundation of the City's approach is its "digital rights" principles. The Mayor's Office of the CTO developed these principles to guide the City's policy, research, programming, and community engagement on core and emerging technologies. Privacy and cybersecurity are central principles, along with Equity, Choice, Affordability, Quality, Accountability, and Ethics and Non-Discrimination.

Recognizing the unique role that cities can play in protecting residents, New York City created the Cities Coalition for Digital Rights in 2018, along with the cities of Barcelona, Spain and Amsterdam, The Netherlands. The coalition, which is managed by the Mayor's Office of the CTO, has since grown to include more than 50 cities worldwide and the partnership of UN Human Rights, UN-Habitat, and other organizations worldwide committed to raising awareness of digital rights challenges, sharing best practices, and advancing policies.

Digital inclusion work – providing literacy training, increasing access, and developing relevant tools – is vital to the City's approach to protecting resident's privacy online. When residents develop skills in navigating the online world and have trusted staff from whom to seek guidance, they increase their safety and privacy online. The Mayor's Office of the CTO's Connected Communities program funds the Library systems and other city agencies to provide digital inclusion resources ranging from classes, to staff support in multiple languages, to facilities with high-speed connections. Last month, the Mayor's Office of the CTO also partnered with the Libraries to host the City's second annual Library Privacy week, which included workshops in every borough in which residents learned how to protect themselves online, and a Privacy Summit for library staff to increase their expertise in supporting patrons in safely engaging online.
This year, the Mayor's Office of the CTO partnered with the City's Cyber Command to engage industry on innovative approaches to address digital rights. The City launched an open innovation challenge focused on enhancing affordable cybersecurity protections for New York's small businesses, which will result in piloting new tools that can increase the security of businesses and the personal information of their customers.

The cornerstone of the City's approach is iterative policymaking that reinforces strong thresholds for privacy and security. In 2018, the Mayor's Office of the CTO created principles for broadband connectivity and in 2019, created the first privacy standards for Public Wi-Fi systems in the country, in partnership with DOITT, Cyber Command, and MOIP.

Mayor's Office of the
Chief Technology Officer

City Legislation on Internet Privacy

In 2018, Mayor de Blasio introduced legislation in the New York City Council to address city residents' portal to the internet, their cable internet service providers. These locally-authorized companies provide the on-ramp to the internet for an estimated 1.8 million New York residents and are the only broadband option for more than two-thirds of our residents.

Currently, cable ISPs, including New York's cable broadband providers, require unlimited release of one's personal information to use what is now an essential service for everyday life. New Yorkers must choose between having privacy or using the internet.

The Mayor's bill would institute the strongest protections of any city in the country. The bill, Int.1101-2018, "Protecting cable provider customers' personally identifiable information," would provide inaugural protections for consumers purchasing internet service from cable companies. The bill would end the unrestricted collection and use of New Yorkers' personal information by cable providers, establish privacy as an essential baseline, mandate true consumer consent to access personal data, limit allowable actions for use of personal data, create transparency in how data is used, and provide remedies for and methods to enforce violations of privacy, including a private right of action.

The City's bill would introduce strong privacy measures including:

- Limiting the data allowed for collection to only data pertinent to service provision;
- Requiring new consent every time data would be used for a new purpose;
- Instituting compliance notifications to the city;
- Preventing fees, punitive pricing, or diminished product quality based upon refusal to consent;
- Requiring strong and transparent notification processes.

State Legislation on Internet Privacy

S. 5642 shares many of the strengths of the City legislation and we are pleased with the direction the Senate is taking. The City encourages the Committees to incorporate the concepts reflected in the City legislation as it considers further development of its online privacy legislation. Additionally, the City encourages:

- Refining the definition of consumers to reflect all household members, not just the subscriber, thereby extending protections to reflect current usage patterns of products and services;
- Incorporating a transparent process for verifying that companies are in compliance with the state's requirements such as annual notifications;

- Clarifying that responsibility for defining categories of eligible exemptions, such as in the public interest, falls to the State;
- Considering further the role of third party data collectors and brokers; and
- Enabling cities to enact legislation that would build upon the state's requirements and address unique local considerations.

The City of New York envisions a better future for our online privacy. The City is pleased that the Committees are charting this path statewide. My colleagues and I appreciate the opportunity to work closely with members of the Senate Committees on Internet and Technology and Consumer Protection on any state privacy legislation.

NYC DOITT
Information Technology & Telecommunications

DEPARTMENT OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS TESTIMONY BEFORE THE NYS SENATE STANDING COMMITTEE CONSUMER PROTECTION AND NYS STANDING COMMITTEE ON INTERNET AND TECHNOLOGY

PUBLIC HEARING: PROTECTING CONSUMER DATA AND PRIVACY ON ONLINE PLATFORMS

FRIDAY, NOVEMBER 22, 2019

Good morning Chairs Thomas and Savino, and members of the New York State Senate Standing Committees on Consumer Protection and Internet and Technology. My name is Michael Pastor and I am the General Counsel of the Department of Information Technology and Telecommunications, also known as DoITT. Thank you for the opportunity to testify today about protecting consumer data and privacy on online platforms. As my New York City colleagues have outlined, this is something that the City is constantly considering across all the work that we do. We applaud the Committees for their attention to this important topic.

DoITT is the largest municipal IT organization in the United States. Our core functions include the delivery of IT services to 100+ municipal entities, including: managing the IT infrastructure and networks (including cloud products), negotiating IT and telecommunications contracts for Citywide use, and serving as the City's telecommunications franchising authority. Our Charter mandate gives us a large responsibility to the public, and privacy is something we consider in everything we do.

As General Counsel, I am deeply involved in the execution of contracts and franchise agreements. New York City has made a purposeful effort to consider privacy in each negotiation and in decision-making on any technology solution. For instance, we negotiate strong security provisions in contracts with vendors that have City residents' data to ensure the confidentiality and integrity of the data, consistent with the privacy principles that my colleague in the Mayor's Office of Information Privacy outlined. Privacy and security are key criteria of public Wi-Fi standards that we developed with MOCTO, so that users of these networks can browse safely without having one's personal information and/or data collected. My team collaborated closely with New York City Cyber Command to procure a mobile application for New Yorkers that alerts them to cyber threats on their phone, including unsafe Wi-Fi networks, all while not infringing on their privacy.

Privacy also underpins our franchise agreements, which we enter with companies who use the public rights-of-way for the delivery of telecommunications services. Our franchises include cable television, mobile telecommunications, and public communications structures (public pay

telephones and LinkNYC). Our focus on privacy carries from negotiation, to execution, and to enforcement for the full term of any agreement. For example, when we entered a franchise agreement for LinkNYC, the City's Wi-Fi kiosk program, we ensured that a strong, enforceable privacy policy was included. This privacy policy prohibits the franchisee from collecting and selling Wi-Fi users' website browsing history and personally identifiable information. We have also closely collaborated with MOCTO on the aforementioned proposed local law to restore privacy protections for broadband customers. This legislation focuses on the cable television franchisees (i.e.: Verizon, Spectrum, and Altice), who provide internet services to the majority of broadband customers across New York City.

As my colleagues have mentioned, we are extremely proud of our work on this legislation and have made efforts to secure its passage in the New York City Council. The New York Privacy Act (S5642/A8526) dovetails with this work, and we are encouraged by the New York State Legislature's consideration of it. We echo the feedback of our colleagues and support the Committees' efforts in moving forward with comprehensive privacy legislation.

Should such a bill pass, it would provide a powerful framework to support all the important work I described earlier. Setting a privacy standard for any prospective vendor or franchisee seeking business with the City will go a long way in supplementing the City's vigilant focus on protecting the privacy of New Yorkers.

Thank you once again for the opportunity to testify today.

###