PARTNERSHIP
for New York City

One Battery Park Plaza, 5th Floor
New York, NY 10004
pfnyc.org

Testimony of the Partnership for New York City

New York State Senate
Senate Standing Committees on Consumer Protection and Internet & Technology

Data Privacy
November 22, 2019

Thank you, Senators Savino and Thomas for the opportunity to testify.

The Partnership for New York City represents the private sector employers of more than 1.5 million New Yorkers. We work together with government, labor and the nonprofit sector to maintain New York's position as the preeminent global center of commerce, innovation and economic opportunity.

We assign great importance to your deliberations on the data privacy issue and the task of creating a framework for how government and business will work together to protect the privacy of personal data, while maintaining a high level of customer service and operational efficiency. New York is a leader in the global innovation economy and in the application of big data. In the absence of federal action, the data privacy standards and procedures that we adopt should be a model for other states and for the nation.

We hope that New York's approach to this legislation will, first and foremost, recognize that data privacy legislation will ultimately impact every business, not just online platforms and social media companies. Moreover, for most businesses, data collection and sharing are intended to improve customer service and security, not to invade customer privacy.

There is general agreement that consumers should have the right to transparency and control over their personal, identifiable data, as distinguished from aggregated or deidentified data or data that is in the public domain. There are differences of opinion, however, even within the business community, as to how privacy protections should be delineated in state law. These differences are reflected in continued debate over the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), both of which have resulted in high costs and major difficulties in compliance and implementation. Just the initial technological and operational costs of compliance resulting from the implementation of the CCPA are projected to be $55 billion, according to a report prepared for the California Attorney General's office. In Europe, it is estimated that the GDPR has resulted in a 33% reduction in the average amount of venture capital funding available for EU tech companies, when compared to funding available to them in the year prior to the GDPR taking effect.

Ultimately, it is important that New York develops legislation that achieves privacy goals without serious collateral damage to our economy. We have reviewed the problems that have arisen in Europe and California, as well as the discussions that are ongoing in other states, to come up with some suggestions for New York to consider in drafting a law that effectively balances consumer and business interests:

- First, the state law should avoid duplication or complication of federal protections where they are in place. Of importance to New York, where the financial services industry is our most important source of economic activity and tax revenues, is to clearly exempt from state regulation those financial institutions that are already subject to strict data security requirements under the federal Gramm-Leach-Bliley Act of 1999. This has not been accomplished in the current draft of the New York Privacy Act (NYPA) which we ask to be amended to exempt institutions rather than data, to avoid unnecessary litigation.
- Second, any law should address the sharing or sale of personal data in a way that provides the consumer with control over how their information is used, but in a manner that is practical and fair. Consumers should have the ability to opt-out of having their personal data sold to unaffiliated third parties for marketing purposes. On the other hand, when data is shared with third parties as an essential element of providing a service the customer wants or expects, or to enhance security or prevent fraud, an opt out provision is not in anyone's interest. Moreover, broad opt-out provisions that severely restrict data sharing or sale will tend to reinforce monopolies, since smaller, third party companies would tend to be restricted from access to data that has been aggregated by large companies. The draft NYPA calls for an "opt in" provision that would be cumbersome for consumers and extremely disruptive for businesses.
- The method of enforcement is ultimately the most important aspect of the law. The best practice in this regard is to authorize the state attorney general (AG) as the enforcement agent. The AG's office has, or can develop, the expertise required to deal with the complexities associated with this emerging area of case law and bring class actions when necessary and appropriate. The most expensive and least effective means of enforcement is through a private right of action, which could inundate companies with individual claims, even for minor technical errors that are likely to be common as new systems for data management and protection are developed. The private right of action should be eliminated from the NYPA; class actions and enforcement should be the exclusive province of the chief legal officer of the state.
- Finally, the NYPA allows only six months for companies to comply with the new law. This is an impossible timeline for many institutions that must convert legacy systems and build new infrastructure to meet the demands of the law. A minimum two-year effective date is a reasonable period to complete the transition.

Over the past two decades, New York companies, academic institutions and government agencies have become leaders in the effective use of data to support business development and job creation, modernization of our health, education and transportation systems, and to improve our environment. To sustain this role requires that we establish a data privacy regime that balances the interests of individual consumers, business, and the general public. We welcome the opportunity to work with the legislature on achieving legislation that both businesses and privacy advocates can champion as we push toward consistent national and global data privacy standards.