The Business Council

Testimony to

The Senate Standing Committees on Consumer Protection & Internet and Technology

RE: Data Privacy

Presented by

Johnny Evers, PhD
Senior Director of Government Affairs

November 22, 2019

Chairman Thomas, Chairwoman Savino, Senators. Thank you for the opportunity to address you today. My name is Johnny Evers, Senior Director of Government Affairs for The Business Council of New York State, Inc. The Business Council is the state's largest business and industry employer association, representing over 2,400 companies. I am also responsible for The Business Council's Information Technology, Telecommunications and E-Commerce Committee. Our IT committee is comprised of hundreds of companies who manufacturing technology products; utilize or engage in technology; operate on the so-called "platform economy"; and create the new digital markets of the 21st century.

Businesses have a responsibility to safeguard data information and prevent its unintentional access or release. We know this to be true. As part of a new digital age, our companies – large and small – have evolved and in many cases re-invented themselves to meet the demands of markets and consumers, and to keep pace with technological advances. Commerce is particularly important in this new world of interconnectivity, with data serving as the intermediary between goods/service and the individual – often in the form of electronic exchange. When consumers place their personal information in the hands of our businesses, they place a trust in these businesses to handle their information safely. But we must keep in mind that the boundaries in the modern world have changed. In reality, today's markets are worldwide. Companies that operate in the most common areas – telecom, e-commerce, banking, insurance, and many others – are accessible via the internet, are no further away than one's cell phone, and consumer goods and products are bought and paid for via electronic debits and credits on personal devices. Thus, to be very clear, we acknowledge the responsibilities we have in regards to privacy and the proper use, storage, and disposal of personal data. Therefore, we recognize the value of regulatory guidelines. Rules governing such massive

areas as finance, banking, communications, indeed all of the free markets, need a carefully thought-out process to insure there aren't unforeseen consequences.

The best way to regulate data privacy is universal federal rules and guidelines. This would be the best, and most logical, source of universal data security standards across all segments of the economy. Such an avenue would insure a consistent set of standards for consumers, a universal and unified enforcement mechanism (quite likely the Federal Trade Commission), and an end to conflicting state rules that foster confusion in regards to data that may (or may not) be subject to multi-state data rules, some of which may conflict with each other. The current multi-state menagerie of rules neither ensures the safety of consumers, nor makes compliance easier for business. In fact, this system may give a false sense of security. It also raises the cost of compliance that, despite its high monetary cost, may also prove specious in regards to security. However, despite its obvious non-partisan appeal, to date there is no definitive consensus at the national level. We sincerely hope this changes in the near future.

As New York State pursues its own course of action in regards to data privacy, any efforts to draft legislation to safeguard data, insure its proper handling, storage and disposal, should include input from the business community. Thus, I greatly appreciate your invitation to appear before you today. By way of example, just this past session The Business Council was very pleased to work with the Legislature and NY Attorney General James and her staff on their proposed "SHIELD Act". In order to provide business input into a growing area of government regulation and oversight in regards to data security, we welcome the opportunity to work with both of your standing committees just as we did on the SHEILD Act.

The SHEILD act is a good example of government and the private sector working together to consult and create a new law to address the issue of data breach. In fact, that bill had been the

subject of well over two years of discussions, conferences, and negotiations among The Business Council, individual member companies, the Office of the Attorney General, and the sponsors. The SHIELD Act provides workable, baseline standards for both security features and notification practices for New York State businesses. Importantly, it recognizes existing standards that are universal for businesses nationwide, often regulated by federal law, with clear reporting mechanisms best suited to protect consumers in New York State.

The SHIELD Act balanced both the state and national rule making paradigm and should serve as template for data protection going forward. Under that act, New York State recognized those existent federal privacy standards in state law and current state regulatory systems (such as those at the Department of Financial Services (DFS)) in the context of a law designed to govern breaches. Numerous existent standards in regards to data privacy such as Gramm-Leach-Bliley, HIPPA, Part 500 of Title 23 of the official compilation of codes, rules, and regulations of New York State, and "any other data security rules and regulations" administered by official departments of federal and New York State governments are recognized under the SHEILD Act. This avoids confusion that would be caused by having businesses and consumers being subject to multiple standards; an outcome that would only serve to complicate the system with no new discernable benefit to consumers. This should be a generally recognized goal of any new state data privacy law – clarity of operations, reporting, and consumer notification.

Just as any efforts to develop a universal standard should strive to insure all data is handled, maintained and stored safely without contradictory rules between the States, so too, the States should strive to insure that laws do not create confusion and aren't diametrically opposed to laws of other States. Anything less would logically lead to regulatory frameworks that prove

unworkable to companies operating within multiple jurisdictions, and just as confusing to consumers. While this is a balancing act – it is not insurmountable.

While I have attempted to lay a certain ground work for the business community in regards to our absolute willingness to provide assistance and input into the process, I want to relay that our Information Technology Committee, comprised of over 500 members, discussed the NY Privacy Act at its recent October 30 meeting in Albany. Our membership includes representatives from large, international technology firms, colleges and universities, health care, telecom, banking and finance, insurance, manufacturing, utilities, computer companies, legal and accountancy professionals, to name but a few. Some of these entities are familiar with the California Consumer Privacy Act since they operate in that state. Likewise, some have working knowledge of the General Data Protection Regulation. While the meeting was informative, it was just a start in regards to studying the issues with eyes towards future input on the topics of data security in New York State generally and the NY Privacy Act specifically.

We have enlisted the help of our members to review the NY Privacy Act with the intent of providing detailed, constructive feedback on the legislation. We believe that as a start, the NY Privacy Act, in its current form, contains some areas that we would very much like to revisit. For example, the bill covers all legal entities that do business in or that sell products and services in New York State, raising some concerns about operations vis-à-vis multiple state operations. The broadness of this implies it has no small business thresholds that may have a disproportionate impact on some entities. The bill covers very broad categories of personal data. It contains an expansive definition of "privacy risk" to include such things as "inconvenience", "unwanted communications", "alters that individual's experiences" or "limits that individual's choices" (Section 1102(2)). The opt-in requirements may lead to very confusing

operations internally. One key issue is the creation of a data fiduciary concept with expressed duties of care and confidentiality to protect individuals from "privacy risk" with legal responsibilities as data fiduciaries superseding legal responsibilities owed to owners and shareholders of the company (Section 1102(3)). Consumer rights to access and to request their own records free of charge up to twice per year, whether deemed excessive or not, would still require untold cost of compliance for what may be limited or non-existent protections. Enforcement by the Attorney General is combined with a private right of action for actual damages and equitable relief.

Though I have touched only on a few parts of the Act, my main point is that we would very much welcome the opportunity to discuss this further and offer suggestions this coming legislative session. Our goal and that of our members who would be subject to the legislation, as both business and consumers, is to help arrive at a final product that can be workable from a business perspective that is also equally cognizant of the consumer concerns and the safeguarding of data. This need not be a mutually exclusive endeavor to the detriment of either partner and we thus offer our help.

Overall, The Business Council appreciates the opportunity to be engaged in this process.