February 09, 2021

Robert F. Mujica
Budget Director, State of New York
NYS State Capitol
Albany, NY 12224-0341

Dear Mr. Mujica:

BSA | The Software Alliance[1] supports a strong, national comprehensive framework that provides all consumers with meaningful rights over their personal data and ensures businesses are accountable for processing that data in line with consumers' expectations. We appreciate the opportunity to connect with you and your staff as you work to provide New Yorkers with transparency and control over their personal data. We wish to serve as a resource by providing our perspective on the different roles that different companies play in protecting consumers' data, as you work to address this important, yet complex policy issue.

BSA is the leading advocate for the global software industry before governments and in the international marketplace. Our members are business-to-business companies that create the technology products and services that power other companies. They offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, and collaboration software. These enterprise software companies are in the business of providing privacy-protective technology products, and their business models do not depend on monetizing users' data. BSA members recognize that companies must earn consumers' trust and act responsibly with their personal data.

BSA and its members have been involved in efforts to strengthen privacy protections throughout the world. At the state level, BSA has most recently engaged with elected officials in California, Virginia, and Washington to ensure privacy frameworks in those states create meaningful rights for consumers and require businesses to handle personal data in ways that consumers expect. Importantly, those rights and obligations must function in a world where different types of companies play different roles in handling a consumer's personal data – making it critical for any privacy law to clearly define those different entities and subject them to strong obligations that reflect their role in processing consumers' data. For that reason, leading privacy laws in the US and worldwide distinguish between the different entities that handle consumers' data and impose strong – but distinct – obligations on them. We urge you to do the same in New York. Specifically, we believe it is critical for any future data privacy law in New York to address:

[1] BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, CNC/Mastercam, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

20 F Street NW, Suite 800
P 202-872-5500
W bsa.org

- ***Definitions of Data Controllers and Data Processors***. Any privacy legislation must define the different types of companies that handle consumers' personal data – and distinguish between those companies that decide how personal data is collected and used ("data controllers") and those companies that process personal data on behalf of other businesses ("data processors"). Both the European Union's General Data Protection Regulation ("GDPR") and California Consumer Privacy Act ("CCPA") incorporate this globally recognized distinction.[2] So, too, do privacy bills under consideration in Virginia and Washington. We recommend the following definitions be included in any future New York privacy legislation:

    - *Controller*. The term "controller" means the person who, alone or jointly with others, determines the purposes and means of processing personal data.

    - *Processor.* The term "processor" means the person who processes personal data on behalf of the controller. A processor should follow the processing instructions of a controller that are agreed to in writing by the parties.

- ***Role-Based Obligations.*** All companies that handle consumer data should be subject to strong privacy obligations – but those responsibilities must be based on the company's role in handling consumer data. For example, companies that decide how a consumer's data is collected and used should be obligated to obtain any consent needed to process the consumer's data. Service providers, in turn, should be obligated to process data on behalf of those other companies and in line with their instructions, so that consumers' data remains protected. In contrast, if service providers were also required to obtain a consumer's consent it could increase consumers' confusion – since service providers may be required to reach out to consumers who don't regularly interact with them. These results can be avoided by adopting the type of role-based responsibilities created by laws like the GDPR and CCPA, which recognize the obligation to obtain a consumer's consent to process data should be placed on the companies that decide why and how to process that data. We also encourage you to look at the Virginia Consumer Data Protection Act, which sets out obligations for data processors that reflect their role in handling consumers' personal data on behalf of other businesses.

As proposed in the Executive Budget, the New York Data Accountability and Transparency Act seeks to provide New York consumers with new data privacy rights and establish the rules by which businesses are to adhere in providing those rights. Unfortunately, the proposal does not distinguish between the different entities that may handle a consumer's personal information or adopt the type of role-based obligations that are foundational to US and global privacy laws. Instead, the proposal would apply in the same manner to any company meeting the definition of "covered entity" – without recognizing the important but distinct role of service providers that process data on behalf of other companies. This approach – of subjecting all companies to the same set of obligations – can create new risks to privacy and security. For example, consumers

[2] For example, the EU's GDPR imposes different obligations on data processors, which handle data on behalf of other businesses, than on data controllers, which decide how and why to collect an individual's personal data. Similarly, the CCPA and now the California Privacy Rights Act ("CPRA") distinguish between "businesses" that decide how data will be collected and used, and "service providers" that process data on behalf of such businesses. The distinction between data processors and data controllers is foundational not only to privacy laws across the globe, but also to leading international privacy standards and voluntary frameworks that promote cross-border data transfers.

should have important new rights in their data, including the right to access, correct, and delete their information. However, if a service provider processing data on behalf of another company were required to provide those rights to consumers, it would create security risks – since service providers interact with the businesses they serve, not the individual customers of those businesses. As a result, service providers generally do not know the individuals who may exercise those rights – and should not be forced to honor requests to access, correct, or delete data from individuals they do not know and whose identity they may be unable to authenticate. Privacy laws that recognize these different roles, and tailor their obligations accordingly, can help avoid these results that would inadvertently undermine consumers' privacy and security.

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these insights. We welcome an opportunity to further engage with you or a member of your staff on these important issues.

Sincerely,

Tom Foulkes
Senior Director, State Advocacy

cc: Beth Garvey, Special Counsel and Senior Advisor
Rebecca Woods, Deputy Special Counsel

20 F Street NW, Suite 800
P 202-872-5500
W bsa.org