November 20, 2020

Harvey Perlman
Chair, Drafting Committee
Collection and Use of Personally Identifiable Data Act
Uniform Law Commission
111 N. Wabash Ave., Ste. 1010
Chicago, IL 60602

Jane Bambauer
Reporter, Drafting Committee
Collection and Use of Personally Identifiable Data Act
Uniform Law Commission
111 N. Wabash Ave., Ste. 1010
Chicago, IL 60602

RE: Feedback of BSA | The Software Alliance on the ULC October 12, 2020, Discussion Draft of the Collection and Use of Personally Identifiable Data Act

Dear Chairman Perlman and Reporter Bambauer:

BSA | The Software Alliance appreciates the opportunity to provide feedback on the Uniform Law Commission (ULC)'s October 12, 2020, discussion draft of its Collection and Use of Personally Identifiable Data Act (the "October Draft"). These comments are intended to supplement the feedback provided by BSA during the ULC's virtual meeting on October 16. While these comments are not intended to address all aspects of the October Draft, we wanted to provide feedback on two core issues confronted by the ULC's drafting committee: (1) the importance of recognizing the roles that data controllers and data processors play in handling consumer data and (2) the broader concerns raised by incorporating aspects of the Alternative Draft into this proposal.

BSA is the leading advocate for the global software industry before governments and in the international marketplace.[1] Our members are enterprise software companies that create the technology products and services that power other businesses. They offer tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, and collaboration software. Businesses entrust some of their most sensitive information — including personal data — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations, and their business models do not depend on monetizing users' data.

I. The October Draft Revises Controller and Processor Definitions in a Manner that Departs from the Global Standard

We are concerned with the October Draft's changes to the definition of controller and processor, which significantly narrow the scope of entities deemed a controller. As we expressed during the October 16

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

meeting, these terms deviate from the global standard – under which an entity is a controller if it determines the *purposes and means* of processing and it is a processor if it processes personal data *on behalf of* a controller. These roles are foundational to privacy laws worldwide, including the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Because a company may act as a controller for some of the products and services it offers (such as those offered directly to consumers) and as a processor for others (such as business-to-business services), it is critical that privacy laws distinguish these two different roles – and clearly set out the obligations for each role.

The October Draft's approach distorts these important roles. The new definition of data controllers only reaches companies that "initially collect[] personal data from or about an individual." (Sec. 2(2).) The definition of data processors has similarly been narrowed, to only those entities that "receive[] authorized access" to certain data covered by the draft law. This new approach alters the relationship between controllers and processors – to the detriment of consumers – in at least two ways:

- First, the new definition of "processor" lumps together two very different types of companies: (1) those receiving data from a controller so they can process data on behalf of that controller and at its direction (e.g., data processors under GDPR and service providers under CCPA), and (2) those receiving data from a controller who can choose how and why to process it for themselves (e.g., other controllers under GDPR and other businesses under CCPA). As a result, the new definition fails to ensure that processors are subject to meaningful limitations in how they use data. In contrast, privacy laws worldwide require processors to act on behalf of and at the direction of controllers – ensuring the obligations placed on controllers to handle consumers' data responsibly flow down to the data handled by processors, as well.

- Second, the narrow definition of "controller" excludes a wide swath of companies that may decide how and why a consumer's data is processed but don't "initially collect" it. For example, it is unclear if data brokers would fall under the new definitions of either controller or processor. By focusing on such a narrow set of entities, the new definition of "controller" meaningfully shrinks the scope of the entire October Draft, without any clear benefit to consumers.

Rather than adopting these new definitions, we recommend the ULC revert to its previous definitions of controller and processor, which align with the international standard found in laws such as the GDPR and CCPA. Not only does aligning the definitions of controller and processor with the global standard increase the ULC Draft's interoperability with other privacy laws – furthering the ULC's goal of fostering uniformity – but it is also important for consumers. By ensuring the ULC Draft reaches broadly to the full set of controllers and processors typically covered by global privacy laws, it helps to ensure that consumers have meaningful rights in personal information processed by those companies and that the obligations placed on companies function in a broad ecosystem in which multiple companies may process consumers' personal data.[2]

II. The October Draft Creates Significant Concerns for Both Consumers and Companies

More broadly, the October Draft incorporates several aspects of the Alternative Draft that create significant concerns for both consumers and for companies. While we greatly appreciate the ULC's effort

[2] For more information regarding BSA's feedback on data controller and data processor issues, please see our March 31, 2020, letter providing comments on the January 7, 2020 discussion draft.

to develop model legislation and the thoughtfulness with which you have approached these issues, we urge the Drafting Committee to reconsider the revised approach reflected in the October Draft, and particularly the draft's approach to compatible uses and voluntary consensus standards.

- *Compatible Uses.* Although we appreciate the October Draft's thoughtfulness in addressing compatible, incompatible, and prohibited uses, we are concerned this approach may not meaningfully advance consumer protections in a manner that is likely to garner widespread support as an alternative to existing privacy frameworks. Indeed, it is not clear that these new sections meaningfully improve the consumer protections created in prior ULC drafts, which reflected many of the rights and obligations consumers may know and expect from other privacy laws.

- *Voluntary consensus standards*. The October Draft's reliance on voluntary consensus standards is also concerning and raises a host of practical difficulties for companies. At the outset, it is not clear that multiple states would adopt the same sets of voluntary consensus standards – reducing the incentive for parties to expend the effort required to create such standards in the first place. If they are developed, though, such standards may ultimately fragment the compliance landscape, particularly when different states adopt different standards that apply to the same set of activities. This fragmentation is especially concerning when these standards are based on a unique approach to privacy laws not reflected in existing global frameworks or international standards.

Ultimately, we believe the novel approach to consumer privacy reflected in the October Draft risks undermining the ULC's goal of furthering uniform state privacy laws, since it is not consistent or interoperable with the approach of existing commercial-facing privacy laws, regulations, or standards, without a clear benefit to consumers.[3] Although we appreciate the importance of creatively examining the complex issues raised by any privacy law, we believe the ULC's previous drafts better achieved the goal of supporting a uniform approach to meaningful state privacy legislation.

We would welcome the opportunity to discuss our comments with you in more detail.

Sincerely,

Kate Goodloe
Director, Policy
BSA | The Software Alliance

[3] For more information on BSA's interoperability concerns, please see our August 12, 2020, letter providing comments on the ULC's Personal Data Protection and Information System Security Act.