April 15, 2021

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 April 2021 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 most recent draft of its Collection and Use of Personally Identifiable Data Act (the "April 2021 Draft" of "CUPIDA"). These comments are intended to supplement the feedback provided by BSA during the ULC's virtual meetings on March 12-13, 2021.

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,

[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., Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

privacy and security protections are fundamental parts of BSA members' operations, and their business models do not depend on monetizing users' data.

While these comments are not intended to address all aspects of the April 2021 Draft, we wanted to provide feedback on two sets of issues. First, we offer specific feedback on language included in the April 2021 Draft. Second, we reiterate concerns we have expressed about the overall approach of CUPIDA, which does not meaningfully advance consumer privacy protections and is not likely to gain the widespread support needed to create a strong alternative to existing privacy frameworks. BSA supports strong privacy protections for consumers and believes individuals should have rights in their personal data; we remain concerned with CUPIDA's approach.

## I. Specific Feedback on the April 2021 Draft

Our specific comments on the April 2021 Draft focus on four areas: (1) definitions of controllers and processors, (2) the role of processors, (3) the treatment of employee information, and (4) enforcement of CUPIDA through existing state consumer protection laws.

**Definitions of Controllers and Processors.** We appreciate the April 2021 Draft incorporating definitions of controllers and processors that move closer to the way these terms are used in existing state and international laws. We encourage the committee to ensure these definitions align with global laws and standards, which both furthers the committee's goal of ensuring a law can be uniformly implemented across states and provides a strong foundation for creating obligations that are tailored to the different roles that controllers and processors play in handling consumers' personal data.

We suggest two ways to improve these definitions:

- Sec. 2(13): Modify definition of processor to account for subprocessors. Processors are currently defined as persons that receive data "*from a controller*." This fails to account for the important role of subprocessors, which are widely used by processors to process data on behalf of a controller. Subprocessors generally receive that data from processors, rather than from controllers, and thus appear to fall outside the current definition. We recommend revising this language to ensure the definition of processors includes subprocessors.

  *Recommendation*: The definition of processor should be revised as follows: "a person that ~~receives from a controller authorized access to~~ processes personal data or pseudonymous data ~~and processes the data~~ on behalf of the controller." This focuses on the key requirement that a processor act "on behalf of the controller."

- Sec. 2(1), 2(22): Eliminate terms "collecting controller" and "third-party controller." We support the ULC's definition of controller, which mirrors the definition of controller included in many state and international privacy frameworks.[2] However, we recommend deleting the further definitions of "collecting controller" and "third-party controller," which are entirely new terms not used in existing

[2] *See, e.g.*, Virginia CDPA Sec. 59.1-571 (defining controllers and processors); GDPR Art. 4 (defining controllers and processors); CPRA Sec. 1798.140 (defining businesses and service providers). For more information about the distinction between controllers and processors, which is foundational to privacy laws worldwide, please see The Global Standard: Distinguishing Between Controllers and Processors in Privacy Legislation, available at https://www.bsa.org/files/policy-filings/03032020controllerprocessor.pdf.

frameworks and have the potential to create significant uncertainty about how obligations for controllers will apply in practice. This formulation also leaves consumers without a right to access data held by a "third party controller" – which significantly narrows the scope of the rights granted to consumers under CUPIDA.

*Recommendation*: Eliminate "collecting controller" and "third-party controller" terms and instead apply all controller obligations to all controllers.

**Role of Processors.** We also suggest three ways in which CUPIDA should be modified to better reflect the role of processors, which process data on behalf of controllers. In many cases, processors have no direct relationships with data subjects and may have limited authority or ability to access the data being processed, which they handle on behalf of a controller. For this reason, privacy laws impose strong – but distinct – obligations on processors, such as requiring them to handle data on behalf of a controller and pursuant to a written contract, as well as requiring adoption of reasonable security measures. We urge the ULC to consider better reflecting these distinct safeguards in the measure by revising Sections 7, 8, and 9.

- **Section 7: Compatible Data Practices.** Section 7(a) clearly states that the compatible data practices set out in CUPIDA apply to both controllers and processors. However, several provisions in Section 7(b) only reference controllers. These should be revised to refer to both controllers and processors.

  *Recommendations:*

  - **Sec. 7(b)(3)** should be revised to include uses that meet a "particular and explainable managerial, personnel, administrative, or operational need of the controller or processor."

  - **Sec. 7(b)(4)** should be revised to include processing that "permits appropriate internal oversight of the controller or external oversight by a government unit or the controller or processor's agent."

  - **Section 7(d)** should be revised to apply to processors: "A controller or processor may process personal data in accordance with the rules of a voluntary consent standard under Sections 11 through 14 ~~to which the controller has committed in its privacy policy~~ unless a court has prohibited the processing or found it to be an incompatible data practice. A controller must commit to such a voluntary consent standard in its privacy policy."[3]

- **Section 9: Prohibited Data Practices.** Section 9 prohibits both controllers and processors from engaging in prohibited data practices, which are defined as acts "likely to" lead to certain results, including specific and significant financial, physical, or reputational harm, misappropriation of identity, or processing data without consent in a manner that is an incompatible data practice.

  This section is likely to create unintended results when applied to processors and may inadvertently undermine privacy and security protections. As the entities deciding why and how a consumers' data is processed, controllers are well positioned to understand if processing is "likely" to lead to the

[3] The requirement to commit to a voluntary consensus standard in a privacy policy only applies to controllers, since processors are generally not consumer-facing and thus are not required under Section 6 to provide a consumer-facing privacy policy.

harms set out in Section 9. In contrast, a processor's role is only to process data on behalf of a controller – and processors often have little authority or ability to access the underlying data, and limited insight into the purposes for which a controller seeks to process data. Prohibiting processors from engaging in actions "likely" to lead to harm could have two unintended results. First, it could cause processors to look at the underlying personal data on their services and review it to independently assess whether the data may be likely to cause harm – thus exposing that data to far more access and diminishing its privacy and security protections. Second, it could cause processors to demand far more information from controllers about the specific purposes of processing and then independently assess whether those purposes are "likely" to lead to harms – upending the traditional relationship between controllers and processors.

We strongly recommend revising Section 9 to better reflect the role of processors by: (1) limiting Section 9 to controllers, and (2) adding to Section 9(c) a provision addressing the liability of processors for actions of controllers, in addition to the current language addressing the inverse scenario of the liability of controllers for actions of processors.

*Recommendations*:

- Section 9(a) should be revised to state: "(a) A controller may not engage in a prohibited data practice, including by instructing a processor to engage in such a practice."

- Section 9(c) should be revised to add a sentence stating: "A processor receiving personal data from a controller or processor in compliance with the requirements of this Act is likewise not in violation of this chapter for the transgressions of the controller or processor from which it receives such personal data."[4]

- **Section 10: Data Privacy and Security Assessments.** This section requires companies to conduct data privacy and security assessments for a wide set of activities – and places that obligation on both controllers and processors, in contrast to many state and international privacy frameworks.

  We recommend the ULC revise the data privacy and security assessment requirement to: (1) place the obligation to conduct assessments on controllers, but not processors, and (2) limit the circumstances in which such assessments are required. This approach would be in line with other privacy laws. For example, Virginia's new privacy law requires controllers – but not processors – to conduct data protection assessments for five specific types of processing activities. Similarly, in California the CPRA requires the state's new privacy regulator to issue regulations requiring businesses – but not service providers – to perform risk assessments. Likewise, the GDPR requires controllers to conduct data protection impact assessments for certain "high risk" activities. Both Virginia's law and the GDPR recognize that processors may need to provide information to a controller for the controller's assessment – but do not require processors to conduct their own assessments. This approach reflects the fact that controllers, not processors, decide how and why data is processed, which are the key features of any risk assessment.

  *Recommendation*: Section 10 should be revised so that only controllers, and not processors, are to conduct data privacy and security assessments. We also recommend limiting the circumstances in

[4] This language is drawn from the Virginia CDPA, Sec. 59.1-578(D).

which assessments are required, to focus on specific activities that may create heightened privacy risks.

**Exception for Employee Data.** As currently drafted, CUPIDA would apply to both consumers' personal data and to the personal data of employees – despite very little discussion within the ULC process about the privacy issues unique to employees, or the consequences of applying CUPIDA's limited access and correction rights to employees. Indeed, the ULC's discussions have overwhelmingly focused on the many privacy issues connected to the collection and use of consumers' personal data, not the personal data of individuals acting in an employment capacity.[5]

This approach is not consistent with the goal of creating a uniform privacy law, because existing state laws have specifically addressed and excluded employees from their scope. Virginia's new privacy law does not apply to employees or those acting as an agent of a controller or processor.[6] In California, the CCPA's application to employees was heavily negotiated and an exception for employee data was extended to 2023 by the CPRA.[7] Many leading privacy bills introduced this year, including those in Virginia, Washington, Minnesota, Connecticut, and Colorado, similarly exclude employment-related information from their scope, given the distinct privacy issues raised by employees and the separate implementation issues posed for employers. We recommend the ULC similarly exclude employee information from CUPIDA.

*Recommendation*: The ULC should adopt an employee exception similar to those in California and Virginia law. The latter excludes: "[d]ata processed or maintained (i) in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role; (ii) as the emergency contact information of an individual under this chapter used for emergency contact purposes; or (iii) that is necessary to retain to administer benefits for another individual relating to the individual under clause (i) and used for the purposes of administering those benefits."[8]

**Enforcement through State Consumer Protection Acts.** Under Section 16, individuals may retain the potential to enforce CUPIDA through a private lawsuit if the state's existing consumer protection act contains a private right of action.[9]

This approach creates very different results for consumers in different states that enact the exact same law, resulting in less uniform enforcement. Nor is it clear that CUPIDA has been drafted to align with existing state consumer protection laws, which may vary in their scope and application to companies in different industry sectors and of different sizes. Moreover, other provisions of CUPIDA contemplate a strong role for the Attorney General, including Section 11, which contemplates a state's attorney general can deem another jurisdiction's law as protective of personal data as CUIPDA and thus treat companies in compliance with that law as compliant with CUPIDA. Similarly, attorneys general are given a central role in recognizing the voluntary consensus standards compliant with the Act. Permitting

[5] This focus may be in part because earlier versions of the ULC's legislative text would not have applied to employees. *See* drafts of April 2020, May 2020, August 2020, and September 2020.
[6] Virginia CDPA, Sec. 59.1-572.C.14.
[7] California CPRA, Sec. 1798.145(m).
[8] Virginia CDPA, Sec. 59.1572.14.
[9] It should be noted that the approach of enforcing CUPIDA through consumer privacy statutes underscores the consumer-facing nature of CUPIDA, as opposed to an employee-facing measure.

individuals to enforce CUPIDA through existing consumer protection acts fragments the enforcement landscape. We recommend the ULC instead ensure a state's attorney general (or other privacy regulator) is the sole enforcement authority, which would better promote a cohesive approach to implementing and enforcing CUPIDA.

## II. Overall Concerns with Approach of ULC Draft

More broadly, the April 2021 Draft retains aspects of the earlier Alternative Draft that create significant concerns for both consumers and for companies, including its focus on compatible uses and voluntary consensus standards at the state level.[10] While we appreciate the ULC's thoughtfulness in approaching issues raised by this model legislation, we continue to have significant concerns about the overall approach now embodied in CUPIDA.

Ultimately, we believe the novel approach to consumer privacy reflected in the April 2021 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 consumer-facing privacy laws, regulations, or standards.[11] Moreover, its variation from those existing laws and regulations does not appear to be driven by a need to protect consumer privacy – which should focus on providing consumers rights in their data and imposing strong obligations on companies to handle data in ways that consumers expect. Although we appreciate the importance of creatively examining the complex issues raised by any privacy law, we believe earlier ULC drafts better achieved the goal of supporting a uniform approach to meaningful state privacy legislation and contained many of the rights and protections consumers may know and expect from other privacy laws.

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

Sincerely,

Kate Goodloe
Senior Director, Policy
BSA | The Software Alliance

[10] *See* Nov. 20, 2020, Letter of BSA | The Software Alliance on October Draft.

[11] Although the ULC has attempted to address concerns around interoperability by treating companies as compliant with the Act if they comply with a "comparable" personal data protection law in another jurisdiction, the revisions to Section 11 allowing attorneys general to charge fees for conducting these assessments only create further confusion under this approach, which could invite attorneys general to routinely opine on Virginia, California, and EU law. Nor are those laws static. For example, in California the new privacy regulator is charged with issuing 22 new regulations by July 1, 2023, that will create new contours around what is compliant with that state's privacy law.