March 31, 2020

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

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

RE: Feedback of BSA | The Software Alliance on
ULC Discussion Draft of January 7, 2020
Collection and Use of Personally Identifiable Data Act

Dear Chairman Perlman and Reporter McGeveran,

BSA | The Software Alliance appreciates the opportunity to provide feedback on the Uniform Law Commission ("ULC")'s January 7, 2020 discussion draft of its Collection and Use of Personally Identifiable Data Act. These comments are intended to supplement the feedback provided by BSA during the ULC's in-person meeting in Washington, DC last month. While they are not intended to address all aspects of the discussion draft, we hope these comments provide you with feedback on a core set of issues confronted by the drafting committee, including recognizing the different roles that data controllers and data processors play in handling consumer data.

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 resources management programs, identity management services, and collaboration software. Our companies compete on privacy—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 data and have long called for a comprehensive national privacy law.

[1] BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, 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.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

Consistent with our feedback at the February meeting, BSA's comments focus on the unique roles of processors and controllers. At the outset, we are pleased that the discussion draft recognizes that processors and controllers are distinct entities, which should both be subject to strong obligations under any privacy law—and that those obligations should be based on their role in handling consumer data. Our comments also focus on other core issues confronted by the drafting committee, including the scope of personal data subject to the act, the treatment of employee information, and enforcement.

I. The Unique Role of Data Processors in Handling Consumer Data

We commend the ULC committee for clearly distinguishing between data processors and data controllers in the discussion draft. This distinction is critical from a privacy perspective, because it ensures legislation can adopt role-based responsibilities that improve privacy protection. Indeed, the distinction between processors and controllers is fundamental to the privacy ecosystem. For example, the EU's General Data Protection Regulation ("GDPR") applies to "controllers" that determine the means and purposes for which consumers' data is collected, and "processors" that process data on their behalf. Similarly, the California Consumer Privacy Act ("CCPA") applies to "businesses" that "determine[] the purposes and means" of processing consumer information and "service providers" that process information "on behalf of" a business. Voluntary frameworks that promote data privacy and cross-border transfers also reflect the distinct roles that different types of companies have in handling consumers' data.[2]

As enterprise software companies, BSA members develop and deliver the technology products and services on which other businesses rely. In this role, they generally act as processors under laws like the GDPR and service providers under the CCPA.[3] Processors are critical in today's economy, as more companies across a range of industries become technology companies—and those companies depend on processors for the technological tools and services that fuel their growth. Software is the backbone of shipping and transportation logistics. It enables financial transactions and remote workplaces all over the world. And it drives the growth of new technologies like artificial intelligence, which have helped companies of all sizes enter new markets and compete on a global scale.

II. The Discussion Draft Should Strengthen the Distinction Between Processors and Controllers And Clarify Their Corresponding Obligations

While we commend the ULC for recognizing the distinction between processors and controllers, we suggest four sets of revisions that would further strengthen this distinction and ensure that each type of entity is subject to strong obligations that reflect its role in handling consumer data.

---

[2] For example, privacy laws in Hong Kong, Malaysia, and Argentina distinguish between "data users" that control the collection or use of data and companies that only process data on behalf of others. In Mexico, the Philippines, and Switzerland, privacy laws adopt the "controller" and "processor" terminology. Likewise, the APEC Cross Border Privacy Rules, which the US Department of Commerce has strongly supported and promoted, apply only to controllers and are complemented by the APEC Privacy Recognition for Processors, which help companies that process data demonstrate adherence to privacy obligations, and help controllers identify qualified and accountable processors.

[3] Of course, when BSA members collect data for their own business purposes, they take on responsibility for complying with the provisions of the GDPR that apply to controllers and the provisions of the CCPA that apply to "businesses" that "determine[] the purposes and means of the processing of consumers' personal information." For instance, a company that operates principally as a data processor will nonetheless be treated as a controller when it collects data for the purposes of providing services directly to consumers.

A. Definitions (Section 2)

The discussion draft currently defines data controllers and data processors separately, but the substance of these definitions departs from the commonly accepted definitions contained in existing legal regimes, without creating a clear benefit to consumers.

Concerns: By departing from widely adopted definitions of controllers and processors used in the GDPR and other existing privacy laws, the discussion draft risks fragmenting compliance efforts, without a clear upside for consumers. Instead of creating new definitions for existing terms, we suggest the ULC further its goal of uniformity by defining controllers and processors in line with the GDPR. The suggested definitions below would also increase consistency with the CCPA's definitions of "business" and "service provider." Because neither the GDPR nor the CCPA incorporate the possession or control test, we recommend that the discussion draft avoid incorporating that test into its definitions. Similarly, we recommend deleting the untested concept of a "data custodian" and instead relying on the existing dichotomy between controllers and processors, which reflects the global standard. Including this new "custodian" term risks fragmentation on a core concept and could signal to companies that they do not need to engage in the essential step as identifying as either a controller or a processor for each activity they undertake.

Recommendation: We suggest the following revisions:

- *Section 2(1):* "Data controller" or "controller" means an entity which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- *Section 2(3):* "Data processor" or "processor" means an entity which processes personal data on behalf of the controller.

- Section 2(2): "Data custodian": We recommend deleting this definition and making corresponding edits throughout the draft.

B. Scope (Section 3)

Section 3 of the discussion draft sets out the scope of the uniform law, including its application to data processors. Under the discussion draft, the uniform law enacted by a state would apply to a company that "is a data processor acting on behalf of a data controller whose activities satisfy the requirements of this section." Sec. 3(a)(3).

Concerns: As written, this provision creates uncertainty for data processors because it would extend the measure to processors that may not know their business customers meet the thresholds for processing and revenue set out in the measure. A processor should only be subject to the law: (1) insofar as it is processing information on behalf of a controller subject to the law, and (2) if the controller has notified the processor that it is subject to the law.

Recommendation: We suggest the following revision:

- Section 3(a)(3): is a data processor, but only to the extent that: (1) it is processing information on behalf of a controller that is subject to the act, and (2) the relevant data controller has notified the processor that it is subject to the act.

C. Duties According to Role (Section 4)

Section 4 of the discussion draft sets out the roles and responsibilities of processors and controllers. We suggest a number of revisions to this section, to better reflect the role of each type of entity in handling consumer data.

1. Scope of Obligations of Data Custodians, Including Processors

Section 4 states that *data custodians* – including both processors and controllers – are subject to five sections of the discussion draft:

- Section 5, Designation of Data Privacy Officer;
- Section 6, Data Privacy Assessment;
- Section 7, Duty of Loyalty;
- Section 8, Duty of Data Security; and
- Section 9, Duty of Data Minimization.

Concerns: Several of these obligations are appropriately placed on all companies that handle consumer data, including controllers and processors. These include obligations to designate data privacy officers (Section 5) and to store data securely (Section 8). However, applying Sections 6, 7, and 9 to data processors raises specific concerns that could ultimately undermine consumer privacy, as set out below.

Recommendation: For the reasons below, we recommend revising the first sentence of Section 4 to state: "A data processor shall be responsible for the duties in Sections 5 and 8."

In particular, applying Sections 6, 7, and 9 to data processors raises the following concerns:

- **Section 6 – Data Privacy Assessment**. This section would require data custodians to complete data privacy assessments of "each processing activity" every two years, including evaluating the type of personal data being processed, the presence of any sensitive data, the scale of processing activities, the context in which data is collected and processed, and the risks associated with the processing, among other information.

  Concerns: Placing this obligation on controllers reflects the fact that controllers make the decisions relevant to such assessments—including deciding whether to collect data, the purpose for its use, and considering the relevant benefits and risks. Processors, in contrast, often endeavor to store data in privacy-protective ways, without looking at its content. Requiring processors to conduct assessments of data they process on behalf of controllers thus undermines privacy, by forcing processors to review data they otherwise would not. That significant intrusion on private consumer data does not have a corresponding benefit to consumers, since controllers should already conduct assessments of data handled by its processors.

  More broadly, even when limited to controllers Section 6 is extremely broad. Unlike Article 35 of the GDPR, which requires data protection impact assessments only for certain "high risk" processing activities, Section 6 appears to require assessments for *all* types of processing. That broad obligation ignores the wide range of processing activities undertaken by companies and the varying effects that processing can have on individuals. Instead, it creates a significant new burden on companies that may decrease their ability to meaningfully assess uses that may carry greater risks.

Recommendation: We recommend revising the discussion draft so that Section 6 only applies to data controllers, in line with the GDPR's requirement that controllers conduct data protection impact assessments.[4]

- **Section 7 – Duty of Loyalty**. This section would prohibit a data custodian from processing or using personal data when processing or use "exposes a data subject to reasonably foreseeable and material risks and harms that are not outweighed by benefits to the data subject or to the public."

  Concerns: Broadly, we are concerned that such an amorphous duty of loyalty may create uncertainty for both business and consumers—at a time when certainty in rights and obligations is particularly important. Indeed, this provision could cut against the ULC's goal of creating a uniform law, by leading to a variety of different interpretations of such a duty by different state courts. In our view, those uncertainties weigh in favor of deleting this provision. To the extent this provision is retained, however, we recommend limiting it to data controllers. Processors simply lack information to understand the risks and harms associated with a particular use of data—because the controller is the entity that determines the context in which data is collected and used, and is therefore aware of the risks involved.

  Recommendation: We recommend revising the discussion draft so that Section 7 is deleted in its entirety. To the extent it is retained, it should apply only to controllers.

- **Section 9 – Data Minimization**. This section would require data custodians not to collect, process, or retain more personal data than necessary to achieve the purposes of processing. For processors, the draft states that when a data controller transfers personal data to the processor, "the controller shall transfer and the processor shall accept only as much personal data as is necessary to complete the processor's processing activities." At the end of the processing, a processor is to destroy all personal data or return it to the controller, pursuant to the contract between the controller and processor required by Section 4.

  Concerns: These requirements create several concerns for data processors. As an initial matter, processors will generally lack sufficient information about a controller's processing activity to be able to understand how much personal data is "necessary" to complete processing activities. Even if a processor had that information, however, its refusal to accept data or its determination that certain data should and should not be processed is fundamentally contrary to its role as a processor—and would require it to make decisions about the "means and purposes," which would transform it into a data controller. This provision accordingly risks disturbing the fundamental distinction between controllers (which decide what data is to be processed) and processors (which process data on the controller's behalf). Instead, a processor's obligation should be to delete or de-identify data after the agreed-upon end of services, or as otherwise directed by the contract between the controller and processor. This helps to achieve data minimization, while preserving the role of data processors as acting pursuant to a controller's instructions.

  Recommendation: We recommend revising the discussion draft so that Section 9 more appropriately reflects the role of data processors. Specifically:

[4] See GDPR Article 35.

- Delete the provision requiring a *processor* to accept only as much personal data as is necessary to complete the processor's processing activities. Instead, the draft's goal of data minimization may be more appropriately achieved by obligating controllers to transfer "only as much personal data is necessary" to a processor in order to achieve the processing activity.

- Revise the final sentence of Section 9, to state: "A processor shall delete, de-identify, or return personal data to the relevant controller at the agreed-upon end of the provision of services, or as otherwise specified by the agreement between the controller and processor required under Section 4."

2. Processor-Specific Obligations

Section 4 also sets out several requirements specific to data processors. We suggest revising these requirements in three ways to better reflect the role of data processors. These changes also increase consistency with existing legal obligations, which furthers the ULC's goal of creating greater uniformity among legal regimes.

- **Section 4(b) – Obligation to Assist Controller**. The discussion draft recognizes that processors "shall adhere to the instructions of the data controller" but broadly requires them to "assist the controller in fulfilling its duties under this [act]."

  Concerns: This broadly worded obligation does not create clarity for businesses that act as controllers or processors. The scope of such assistance may therefore vary considerably between different states enacting the model legislation, which could have significant downsides for consumers—particularly because the current draft fails to specify the assistance a processor must provide to a controller in responding to consumer rights requests. We recommend adopting specific language drawn from the GDPR, which requires processors to create "technical and organizational measures" that help the controller respond to consumer rights requests.

  Recommendation: Section 4(b) should be revised to state: "A data processor shall adhere to the instructions of the data controller and shall, taking into account the nature of the processing, assist the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to consumer rights requests under this act."[5]

- **Section 4(c) – Prohibition on Processing For Purpose Not Included in Consumer Notice**. The discussion draft would prohibit processors from processing personal data "for any purpose that was not included in the notice provided to data subjects by the data controller as required by this [act]."

  Concerns: Data processors do not receive the notice provided to data subjects—and are generally not told by controllers of the specific purpose(s) of each type of processing they undertake. For example, a cloud storage provider may store a company's data without understanding if the data includes only employee records, or only consumer records, or both. Processors therefore lack the information needed to understand if the processing activity they are performing was included in the notice provided to data subjects or not. If processors were required to make that determination, it would both: (1) force them to look at the content of records they

[5] This language is drawn from GDPR Article 28(3)(e).

otherwise would not, undermining privacy protections, and (2) require them to make decisions about what data should and should not be processed—thus transforming them into a controller, rather than a processor. Moreover, this provision is not needed to further consumer privacy, because Section 11 already requires controllers to only process data for purposes consistent with the notice provided to consumers. This obligation already protects data handled by processors, since processors only handle data on behalf of a controller and consistent with their instructions.

Recommendation: We recommend deleting Section 4(c).

- **Section 4(e) – Engagement of Subcontractors**. The discussion draft would prohibit data processors from transferring personal data to another processor unless it has the "express written consent" of the controller and the transfer is governed by a written contract that "imposes all the same obligations" on the recipient that are imposed on the processor, regardless of whether the recipient is otherwise subject to the Act.

  Concerns: We recognize that it is critical for obligations placed on processors to flow down to subprocessors. At the same time, obligations to obtain the express written consent of a controller to engage a subprocessor risk overwhelming both controllers and processors with new notices and contract terms, given the substantial volume of subprocessors used by many businesses. Instead of requiring express written consent, we encourage the ULC to require controllers be provided with an opportunity to object to the use of subprocessors. This ensures controllers may refuse subprocessors in certain contexts, while providing flexibility to both entities.

  Recommendation: Section 4(e) should be revised to state: "A data processor shall engage a subprocessor only after providing the controller with an opportunity to object and pursuant to a written contract in accordance with this section, which requires the subprocessor to meet the obligations of the processor."

D. Other Provisions Inconsistent with Role of Data Processors (Section 11, Section 12(c))

Several portions of the discussion draft also contain provisions that are inconsistent with the role of data processors, which handle data on behalf of controllers. Below we set out recommendations to two such provisions.

- **Purpose Limitation (Section 11)**. The discussion draft would require a controller not to process data for a purpose not specified in the notice to data subjects. In addition, the draft states a controller shall not "permit processors or other persons" to process data for such purposes.

  Concerns: This provision raises at least two concerns, including not reflecting the role of processors in handling consumer data.[6]

  - *Role of processors*. The current language prohibiting controllers from "permit[ing] processors" to process personal data for certain purposes does

[6] Section 10(b) would also require controllers provide consumers with a telephone number to contact to exercise their rights under the model legislation. That requirement is inconsistent with many business-consumer relationships, which may occur entirely online. We recommend modifying this provision, to require a phone number be provided only if the controller does not provide an online contact method.

not fully reflect the role of processors—which act on behalf of a controller. To the extent this clause is retained, we suggest revising it to clarify that a controller "shall not instruct a processor" to process data for purposes inconsistent with the purposes contained in the notice to a consumer, or as otherwise permitted under the Act. This helps achieve the goal of ensuring that a controller handles data in line with notice provided to consumers, while reflecting that a controller's role is to provide instructions to processors.

- *Focus on purpose specification*. More broadly, we support the views expressed at the February meeting that this provision should be revised to focus on purpose specification, rather than purpose limitation. The existing language would create liability for a controller that processes data for a purpose "not specified" in the notice to consumers. That creates an incentive to over-notify users, resulting in longer and less useful disclosures to consumers. Instead, we recommend re-framing this provision to focus on purpose specification and require controllers to act in a manner that is consistent with that notice. At the same time, we recognize that controllers may seek to use data in a new way, not consistent with the notice provided to consumers—and support requiring affirmative express consent for such situations.

Recommendation: We recommend revising Section 11 to state:

Purpose Specification

(a) A controller shall inform consumers of the purposes for which it collects and uses personal data.
(b) A controller shall use personal data in a manner that is consistent with that explanation, the context of the transaction, or reasonable expectation of the consumer, or in a manner that is otherwise compatible with the original purpose for which the data was collected. A controller shall not process personal data for a purpose that is materially different from the purposes for which the data was initially collected or subsequently authorized by the affected consumers, unless the controller obtains affirmative express consent prior to such additional processing.

- **Role of Processors in Responding to Data Subject Rights Requests (Section 12(c)).** The discussion draft requires controllers to make reasonable efforts to ensure that its responses to consumer rights requests include personal data in either their possession or control or "in the possession or control of data processors acting on the controller's behalf." Moreover, the controller "shall make reasonable efforts to notify processors acting on its behalf when a data subject exercises these rights, and shall instruct the processor to comply in the same fashion as the controller."

  Concerns: This provision could undermine consumer privacy, by potentially requiring data processors to respond directly to consumer rights requests. That obligation to interact with consumers and determine the validity of their rights requests falls on controllers; processors should be obligated to provide a controller with the technical and organizational measures needed to respond to such requests itself, in line with Article 28 of the GDPR.

Laws like the GDPR and CCPA require controllers to respond to consumer rights requests, because controllers interact with consumers and decide when and why to collect their data. Moreover, controllers must decide if there is a reason to deny a consumer's request, such as when a consumer asks to delete information subject to a legal hold. Processors, in contrast, often do not know the content of the data they process, and may be contractually prohibited from looking at it. It is not appropriate for processors to respond directly to a consumer's request—which creates both security risks (by providing data to consumers they do not know) and privacy risks (by looking at data they otherwise would not). Processors should instead provide controllers with tools the controller can use to collect data needed to respond to a consumer's request.

Recommendation: We recommend deleting the second sentence of Section 12(c) ("The data controller shall make reasonable efforts to notify processors acting on its behalf when a data subject exercises these rights, and shall instruct the processor to comply in the same fashion as the controller"). No additional language needs to be added here to ensure that processors provide a controller with the appropriate technical and organizational measures for the controller to respond to consumer rights requests, because that obligation would be imposed by our suggested revisions to Section 4(b), above.

III. The Discussion Draft Should Further Clarify Obligations for Businesses and Rights for Consumers

In addition to clarifying and strengthening the role of processors and controllers under the discussion draft, we believe the discussion draft should be revised in at least six additional ways to further protections for consumers and clarify obligations on businesses.

A. Definitions (Section 2) – Scope of Personal Data and Treatment of Employee Information

Concerns: The broad definition of personal data extends well beyond information relating to consumers. We recommend revising several definitions to ensure the discussion draft focuses on privacy protections for consumers—and does not extend to information about households or devices. In addition, the definitions should ensure that employee data is excluded from the definition of personal data, as employee data raises distinct privacy issues that are addressed by a range of other state-level laws, including employment laws.

Recommendation: We recommend narrowing the definition of Personal Data to focus on information relating to an identifiable individual. In addition, the definition should be clear that the individual is a "consumer" and not an employee. Specifically:

- The definition of Personal Data in Section 2(9) should be revised to state: "Personal data means any information relating to an identified or identifiable consumer. An identifiable consumer is one who can be identified, directly or indirectly, through reasonable effort by the controller with the information to which it has access, by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, or genetic identity of that consumer."

- The draft should add a definition of Consumer: "Consumer means a natural person. A natural person is not a consumer to the extent that the person is acting as an

employee, owner, member, or other contractor of a partnership, corporation, trust, estate, cooperative, association, or other entity."

- The definition of Data Subject in Section 2(4) should either be deleted or modified to reflect the changes recommended above. If the definition is retained, we recommend modifying it to state: "Data subject means the consumer to whom personal data refers."

B. Data Subject Rights (Section 12)

Any comprehensive privacy legislation must create important rights for consumers, including the right to access, correct, and delete information. BSA therefore supports including these rights in the discussion draft, but recognizes the committee must refine the draft to ensure that consumer rights are not exercised in a manner that ultimately undermines privacy or security.

Concerns: The discussion draft does not currently address exceptions to consumer rights requests. The draft should take care to create a thoughtful and reasonable set of exceptions to consumer rights requests, to ensure companies are not required to honor requests that may ultimately undermine the privacy and security of consumers.

Recommendation: We recommend creating a new section within the discussion draft that creates exceptions to consumer rights requests. For example, several federal proposals for comprehensive privacy legislation recognize a number of exceptions to consumer rights requests, such as when a consumer's identity cannot be verified, compliance is contrary to a legal obligation, fulfillment would undermine an individual's privacy or safety, the data is needed to detect and respond to security incidents or protect against malicious or legal activity, or is needed for certain internal uses, such as repairing and improving products.[7] As those measures recognize, these exceptions may appropriately differ when responding to different types of consumer requests (e.g., access, correction, or deletion), or may overlap with exceptions to consent requirements.[8]

C. Non-Discrimination (Section 17)

The discussion draft contains a provision similar to the CCPA, which prohibits a controller from discriminating against any data subject for exercising rights under the act, "including by denying goods and services, charging different rates, or providing a different level of quality, except that a data controller may provide benefits to data subjects that are closely related to the purpose of processing and that require access to personal data."

Concerns: The similar CCPA provision has already created a great deal of uncertainty for both businesses and consumers. Replicating that provision in the discussion draft creates tension with the ULC's larger goal of supporting uniformity, because it is another provision that may lead to inconsistent outcomes when applied in different states. Substantively, the concerns about varied applications among states are underscored by the lack of clarity about

[7] House Energy and Commerce Committee Staff Discussion Draft, § 5(b), 116th Cong., (2019); United States Consumer Data Privacy Act of 2019, § 108 116th Cong. (2019) (Staff Discussion Draft); Consumer Online Privacy Rights Act, S. 2968, § 110(a),(c) 116th Cong. (2019).
[8] United States Consumer Data Privacy Act of 2019, § 108 116th Cong. (2019) (Staff Discussion Draft). (setting out a list of exceptions pertaining to both consumer rights requests and to consent requirements).

how the provision would apply, including to businesses that provide personalized recommendations but could not do so for individuals who decline to provide their data.

Moreover, this provision is also not needed, since the discussion draft reflects a comprehensive approach to privacy that creates a range of rights for consumers and obligations on businesses—in stark contrast to the CCPA. The need for such a provision is therefore reduced in this context, and in our view the negative consequences of including it outweigh the potential benefits.

Recommendation: We recommend deleting Section 17.

D. Profiling (Section 2(11), Section 14(a))

The discussion draft provides data subjects the right to opt-out of processing and transfers for purposes of "profiling in furtherance of decisions that produce legal effects or similarly significant effects concerning the data subject." (Section 14(a).) Profiling, in turn, is defined as "any form of automated processing of personal data to evaluate, analyze, or predict a data subject's economic status, health, demographic characteristics (including race, gender, or sexual orientation), personal preferences, interests, character, reliability, behavior, social or political views, physical location, or movements." It does not include "evaluation, analysis, or prediction based solely on a data subject's current activity, including search queries, if no personal data is retained for future use after the completion of the activity." Further, "[p]robabalistic inferences derived from profiling are personal data."

Concerns: While this provision appears to draw inspiration from Article 22 of the GDPR, it is far broader and appears to provide a consumer the right to opt-out of all automated processing, rather than a right to human review of decisions based solely on automated processing, as in the GDPR. Moreover, the draft does not set out exceptions to any such right, including when the processing is necessary to perform a contract with the consumer or otherwise provide a requested service. Nor does the draft define what "legal effects" means—which once again may create considerable uncertainty about the scope of its application across a range of states.

Recommendation: We recommend deleting the right to opt-out of profiling from Section 14(a)(2), and deleting the corresponding definition of profiling in Section 2(11).

E. Private Right of Action (Section 20)

The discussion draft contains a private right of action, which attaches to eight sections of the bill and would allow recovery not only of actual damages but also statutory damages.

Concerns: BSA believes all privacy laws should be strongly enforced, but a private right of action is not required to create effective and strong enforcement. Rather, a strong, central regulatory approach—with the state attorney general as the enforcement authority—is the best way to develop sound practices and investment in engineering that protects consumers. State attorneys general have a strong track record of enforcing privacy-related laws—and do so in a manner that creates effective enforcement mechanisms while providing consistent expectations for consumers and clear obligations for companies. Moreover, empowering state attorneys general to enforce a new privacy law ensures that enforcement rests with an agency that can observe the principle of bringing cases that remedy and deter harmful conduct, rather than punishing technical lapses. We believe that if states enact new comprehensive privacy laws, they should be enforced by the state attorney general—which should be provided with the tools and resources needed to carry out its mission effectively.

Recommendation: We recommend deleting Section 20.

F. Effective Date (Section 24)

The discussion draft anticipates that the measure would take effect 180 days after enactment by a state legislature.

Concern: A 180-day transition period is not enough for the wide range of companies that would be subject to a comprehensive privacy law to understand their obligations under the law and operationalize them.

Recommendation: Any bill enacted as a result of the ULC process should not take effect until companies have had sufficient time to ensure they are in compliance with the requirements of that bill. We recommend ensuring a two-year transition period, which is consistent with the GDPR's two-year transition period and would enable companies to design compliance solutions that meaningfully implement the measure's requirements.

* * *

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these comments. We welcome an opportunity to further engage with the ULC committee on these important issues.

Sincerely,

Kate Goodloe
Director, Policy
BSA | The Software Alliance