April 19, 2021

Mr. Harvey Perlman, Chair
Ms. Jane Bambauer, Reporter
ULC Collection and Use of Personally Identifiable Data Committee
Uniform Law Commission
111 North Wabash Ave.
Suite 1010
Chicago, IL 60602

Dear Chair Perlman and Reporter Bambauer,

Internet Association ("IA") appreciates the opportunity to provide comments to the Uniform Law Commission's ("ULC") Collection and Use of Personally Identifiable Data Committee ("Committee") on the most recently proposed uniform law on data privacy, the "Uniform Personal Data Protection Act" ("UPDPA/April 2021 draft/the model Act"). IA looks forward to participating in the April 23 virtual meeting and would be happy to provide further explanations or drafting suggestions related to the feedback, below, during the meeting or following it.

As we continue to see many states introduce consumer privacy focused legislation, IA member companies have consistently advocated for alignment amongst state privacy proposals and would ultimately like to see comprehensive federal privacy legislation passed this year. It is important for U.S. consumers and businesses of all sizes to be able to rely on consistent nationwide privacy standards that include clear and reasonable compliance guidelines. In particular we would recommend that the Committee align its April 2021 draft with emerging state privacy laws such as the Virginia Consumer Data Privacy Act ("VCDPA").[1]

While these comments do not encompass all of IA's concerns with the April 2021 draft, they do recognize specific provisions where we feel change is needed to create a more uniform piece of model legislation. More generally we do have concerns about how the Committee's April 2021 draft continues to diverge from leading state and international privacy laws in scope, framing, and terminology. IA members support the Committee's goal to put forth unifying model legislation that both protects consumers and provides effective guidance for businesses. However, in its current form the April 2021 draft contributes to the developing patchwork privacy landscape of fragmented and uncertain privacy rights and standards across the United States.

[1] Virginia Consumer Data Protection Act (CDPA) §§ 59.1-571- 59.1-581 (2021).

IA's members are supportive of meaningful privacy rights and controls for consumers, but UPDPA's approach does not seem to be the best path forward both because of jurisdictional differences it encourages across states and its deviation from existing standards and requirements. The following are some of the areas that IA would like to particularly note are of concern:

Enforcement Under State Consumer Protection Acts: IA would recommend that the Committee adopt exclusive Attorney General (AG) enforcement for violations of the model Act. Allowing for an indirect or direct form of a private right of action (PRA) to carry out the provisions of the model Act will not benefit consumers in an effective manner and will cause costly litigation for all parties involved. Under Section 16 of UPDPA, the Committee defers to the state's consumer protection act, which can vary widely amongst states and frequently include an extensive PRA. As a result, a confusing patchwork of enforcement regimes and case law arises -- making compliance across multiple states increasingly difficult. Consumers are better served by clear rules that businesses are able to follow and enforcement mechanisms that are designed to deter violations of such rules and result in appropriate compensation to consumers where they have incurred a loss.

Exclusive AG enforcement allows an experienced entity like the AG's office to identify companies acting in bad faith towards their consumers' privacy rights and ensure that proper measures are taken to protect all consumers' privacy rights. Conversely, a PRA rarely benefits a consumer in the way it is intended -- especially when it comes to expensive and prolonged class action lawsuits -- the plaintiffs attorneys are often the only individuals that receive large payouts with consumers receiving token amounts for their alleged injuries. Given the high cost of litigating class actions, settlements are frequent and simply a cost-effective solution for the defendant. They provide no insight into whether the challenged conduct actually constitutes a legal violation.

Other states that have passed or are considering comprehensive privacy legislation this year and recognize the value of AG enforcement. For example, Virginia adopted an exclusive AG enforcement approach under the VCDPA; Connecticut's proposed privacy act (SB 893) also provides exclusive AG enforcement; and Washington state's Senate Privacy Act (SB 5062)(the only version of the WPA to pass a chamber this year) also limits enforcement to the AG. As a result, the Committee should follow suit and include an exclusive AG enforcement mechanism within the UPDPA model legislation.

IA would also encourage the Committee to include a "right to cure" to Section 16's enforcement provision to allow businesses to have the opportunity to cure alleged consumer rights violations. This would provide businesses with an opportunity to quickly resolve consumer concerns and establish a more solid foundation of consumer trust.

We would encourage the Committee to consider two proposals under Section 16(b), which allows the AG to create future rules and regulations under the April 2021 draft. IA would recommend there be a refined scope for the AG's authority to promulgate these regulations, specifically we would suggest technical fixes when necessary. If regulatory authority remains broad, IA would encourage adding a requirement for these regulations to be completed at least one year in advance of the Act becoming effective. Such a provision would allow companies to build out their systems in compliance with the all requirements in place as opposed to having to restructure their system once the AG releases new regulations.

Finally, IA would ask that under Section 16(a) where there is a violation of the Act, only the AG only be allowed to bring an action under this model Act and that the action be capped to statutory damages recognized under the April 2021 draft.

Preemption: Under Section 17 of the April 2021 draft it states "th[e] Act does not create, affect, enlarge, or diminish any cause of action under the law of this state other than this [act]." This language seems to indicate that a resident of the state can bring a violation of the model Act under another state act, if the act is pertinent to the violation. However, IA would recommend that violations of the model Act are solely brought under the Act itself and the Committee not allow for alternative actions to be brought under other acts in the state.

Effective Date: IA would strongly encourage the April 2021 draft to include an effective date that is *at least two years* after the law has passed. The current proposal of 180 days with a potential 60 day extension for compliance is not sufficient time for businesses to come into compliance with the Act. IA would also recommend that all AG regulations that pertain to the Act be finalized at least one year prior to the Act's effective date.

Controller-Processor Distinction: IA would also recommend that the definition of controller and processor be consistent with existing U.S. and international standards contained in the VCDPA and the EU's General Data Protection Regulation ("GDPR").

- **Controller Definition Recommendation**: There is no need to make further distinctions between "collecting controller" or "third party controller", if the *controller* is defined as "*the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data*."[2]

- **Processor/Processing Definition Recommendation**: Furthermore, the definitions of "processing" and "processor" should also be consistent with the GDPR and VCDPA precedent. *Processing* should be defined as "*any operation or set of operations performed, whether manual or by automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or*

[2] Virginia CDPA, § 59.1-571(defining controller).

modification of personal data."[3] In turn, a *processor* should be defined as "*a natural or legal entity that processes personal data on behalf of the controller.*"[4] Additionally, by including the "maintains" definition, there creates further confusion between the roles of controllers and processors and does not provide businesses with clear guidance on how to classify themselves under the April 2021 draft.

IA would also recommend that the Committee provide guidance for both controllers and processors based on their respective relationships with consumers personal data. It is important that any model legislation acknowledge the different parts of handling consumer's personal data and implement administratively feasible requirements for each. For example, under Section 7: Compatible Data Practices, the April 2021 draft states "a controller or processor may engage in compatible data practices without the data subject's consent[,]" however under Section 7(b)(2)-(4) only a controller's compliance with a legal or regulatory obligation; personnel, administrative, or operational need; internal oversight; or external oversight by a government unit apply only to the controller when the processor could also be subject to these activities. As a result, we would suggest including these activities as compatible data practices for *both processors and controllers*.

Finally, since the GDPR's effective date the law's definitions of controller and processor have sufficiently allowed companies to distinguish their roles in handling individual's personal data. The recently enacted VCDPA uses an extremely similar distinction between controllers and processors to provide companies with a familiar and useful framework that allows for companies to more quickly come into compliance with the law.

Personal Data Definition: IA would also encourage the Committee to adopt a broader definition of personal data that is consistent with the VCDPA, and the GDPR. As a result, the model Act would be able to work within a variety of modern data sets that will have lasting privacy implications. By including additional definitions such as "data'', there creates uncertainty as to what information may be subject to specific provisions of the law and ultimately creates compliance and clarity concerns for businesses and consumers alike. IA would also recommend that the definition of personal data not include pseudonymised data. Based on the requirements in this model Act, it would be difficult for companies to comply with requests of pseudonymised data from consumers, and asking for businesses to reidentify pseudonymized data for the purposes of access or correction seems overly burdensome and creates unrealistic expectations of businesses.

[3] Virginia CDPA, § 59.1-571(defining processing).
[4] Virginia CDPA, § 59.1-571(defining processor).

Pseudonymized Data Definition: IA would also suggest that the Committee align the definition of pseusonymized data with the definition "pseudonymous data'' contained in the VCDPA. As currently drafted, the definition seems to compete with the definition of personal data. Furthermore, this is consistent with the April 2021 draft's provisions under Section 5 that do not require the same requirements for pseusonymized data and personal data when it comes to access and correction.

- **Pseudonymous Data Definition Recommendation**: *"[D]ata that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person."*[5]

Employee Data Exception: As currently drafted the model Act would apply to both consumer's personal data and an individual's personal data in the employment context. During the Committee's meeting discussions and in previous drafts, the Committee seems to focus on an individual's personal data in the consumer context. Additionally, the California Consumer Privacy Act ("CCPA")/California's Privacy Rights Act ("CPRA") and VCDPA both include an exception for employee data. Furthermore, several privacy proposals this year including Washington state and Connecticut have also contained an employee exception. In order to create a more consistent privacy landscape, IA would suggest the Committee adopt the employee exception contained in the VCDPA[6] in the April 2021 draft.

Incompatible Data Practices: As we noted at the beginning of our comments consistency amongst privacy proposals is key to allowing businesses to quickly come into compliance with the law. Currently, no modern privacy laws include an "incompatible data practices" section, therefore IA would recommend eliminating this provision of the April 2021 draft. However, if the Committee moves forward with this provision IA would recommend the following changes:

- **Section 8(a) Recommendation**: The text states, "[p]rocessing is incompatible if it contradicts or is not disclosed in the privacy policy," however, the explanatory comment indicates that the incompatible processing will be subject to a harm/benefit assessment, which conflicts with the original text. Therefore, IA would strongly encourage the Committee to eliminate the comment and keep the actual text of the April 2021 draft.

[5] Virginia CDPA, § 59.1-571(defining pseudonymous data).
[6] Virginia CDPA, § 59.1-572 (C)(14).

Prohibited Data Practices: Section 9 prohibits both controllers and processors from engaging in prohibited data practices. Section 9(a) then goes on to define a “prohibited data practice” as “processing personal data in a manner that is “likely to” cause things like financial, physical, or reputational harm, undue embarrassment; assumption of another’s identity; violations of a federal or state law outside of this Act; etc. However, many of items on the list of prohibited data practices fall under existing state or federal law (e.g. Fair Credit Reporting Act), so this Section seems to be redundant and, given the lack of adequate definitions or standards for the other harms to determine whether something rises to the level of being a prohibited practice, could cause confusion for businesses trying to comply with the model Act. Therefore, IA would recommend eliminating this provision for the April 2021 draft.

Compliance with Other Data Protection Laws: In prior UPDPA drafts, there was a provision that stated if a business was already compliant with laws such as CCPA/CPRA or the EU’s GDPR that they would be exempted for the requirements of the model law. However, in this new draft it seems that the AG will be able to charge businesses a “reasonable fee” to investigate whether he/she thinks that the law the business is compliant with meets an unknown privacy standard of the state. First, this method does not allow for consistent application, while one AG may feel that the GDPR sufficiently protects consumers another AG may feel that the law is overly strict or does not go far enough. Moreover these decisions as to the adequacy of other privacy regulations are not specific to any one business and it would alleviate burdens for businesses and the AG offices to simply establish a list of pre-reviewed privacy regimes and allow business petition for review of regimes that were not evaluated in the preparation of that list. Instead, IA would suggest that if a business is already in compliance with the CCPA, GDPR, or one of the many federal privacy laws included in Section 11, they will be exempt from this law’s requirements.

Privacy Policy Requirements: IA would also recommend eliminating the requirement that a controller include a “voluntary consensus standard the controller has adopted and complies with” in its privacy policy. Although the April 2021 draft provides states to allow for the creation of voluntary consensus standard bodies, the state is not required to do so. Therefore, it seems reasonable that a company not be required to include this information in its privacy policy.

While we appreciate the Committee’s efforts to incorporate many stakeholders’ feedback into its most recent draft, IA believes that there are many further changes and adaptations that need to be made to this proposal prior to its release and we would encourage the Committee to continue these meetings until there is more clarity within the law. IA would also encourage the Committee to look to more recently enacted privacy laws such as VCDPA to allow for consistent consumer privacy expectations across the United States, as opposed to a patchwork of state privacy laws that will create confusion.

We thank you for the opportunity to provide our feedback and look forward to working with the Committee to find ways to create consistent and effective privacy laws throughout the United States.

Sincerely,

Alex McLeod

Alexandra McLeod
Legal and Policy Counsel
Internet Association