Comments of Internet Association: CUPIDA April 21 Draft

Internet Association ("IA") appreciates the opportunity to provide feedback to the drafting committee on the most recent draft of the proposed uniform law on data privacy, the "Collection and Use of Personally Identifiable Data Act."[1] IA looks forward to participating in the April 24 virtual meeting and would be happy to provide further explanations or drafting suggestions related to the feedback, below, during the meeting or following it.

At this stage of the drafting process, IA would like to highlight the following points:

- **Risks of different implementations by states:** In order to avoid a patchwork approach across states, the draft should limit, to the extent possible, the provisions which are likely to result in state-by-state variations, including broad rulemaking mandates to state attorneys general and interpretations of the uniform law by state courts through a private right of action. In addition, to avoid duplication of efforts by state attorneys general, it would be helpful to have a mandatory coordination mechanism for state AGs to work jointly on specific cases enforcing the uniform law. This would also help spread the burden of enforcement across AG offices, enhancing AG enforcement capabilities and minimizing unintended divergence in enforcement decisions, while minimizing risk covered entities facing multiple AG inquiries on the same matter.
    - **Regulatory Enforcement:** Section 19 of the draft should be reviewed as the draft develops and refined to only authorize attorneys general to issue regulations that are necessary for implementation of the uniform privacy law. IA appreciates the addition of considerations for AGs in developing regulations, including consistency across states, but still views targeted rulemaking as essential to limit divergence among states.
    - **Private Right of Action:** IA shares the concerns of other commenters that a private right of action creates significant controversy because of the regulatory uncertainty it introduces, the emphasis it creates on fulfilling technical requirements over more substantial privacy enhancing investments, and the lack of transparency that results from settlements, including whether laws have been violated and to what extent victims have actually been compensated for the alleged harms.
        - Regulatory uncertainty is a significant concern. IA believes that Section 20's private right of action ("PRA") will result in varying interpretations of the obligations of the privacy law. While IA appreciates that the intent was for the private right of action to be narrow and apply to clear statutory requirements, IA is concerned that, as written, it remains too broad to avoid creating a complex and disparate body of case law interpreting the

[1] IA is providing comments on the most recently circulated redline of CUPIDA received on April 21. IA also mentions text from prior drafts for purposes to share perspective on why recent changes are helpful.

uniform law. Even if the drafting committee is able to narrow the provision, IA believes that private litigation will nonetheless push the boundaries, because of the incentives to focus on cases that can provide the greatest financial award, rather than the clearest violations. For example, though CCPA has a narrow private right of action for data breaches in Cal. Civ. Code § 1798.150, class action lawsuits have already been filed under CCPA alleging a broader range of harms. *See, e.g.*, *Cullen v. Zoom*, Case No. 5:20-cv-02155-SVK, N.D. Cal., filed March 30, 2020. For this and the other reasons mentioned, IA advocates striking the PRA and considering alternative consumer remedies. As noted, despite the CCPA's narrow private right of action, which also includes a requirement to give notice and an opportunity to cure before filing suit, these efforts to limit and narrow when private suits may be brought are already ineffective.

- **Duty of Loyalty:** Section 9 of the draft proposes to give state attorney generals the authority to issue regulations to which practices are "abusive"-- an undefined term. This will inevitably result in varied approaches across the states that would adopt the ULC law. In addition, these types of provisions which attempt to import concepts from other areas of law are novel, unproven, and unpredictable. IA's recommendation is that this entire section be struck from the draft or that the provision be reformulated and tied to the risk assessment requirement.
  - IA notes that none of the leading global privacy standards incorporate the concept of a duty of loyalty or any type of fiduciary relationship between the data subject and the data processor. Instead, the existing standards set forth rules for engagement based on long standing principles for processing personal information, including transparency, access, deletion and control. In addition, no recent proposals that would create a duty of loyalty or a fiduciary relationship in the context of privacy law have been enacted in law. (*See, e.g.,* the proposed New York Privacy Act (S.5642), and U.S. Sen. Schatz' proposed Data Care Act (S. 2961). These types of provisions are controversial and have not gained traction, in part because they include vague and undefined terms, like "abusive," which fail to give the entities subject to the requirements adequate warning of what behaviors are allowed and which are not. AG regulations could solve this problem, but will inevitably result in wide variations among states because of the wide discretion inherent in a provision that functions as a catch all. The draft does not give any direction or guardrails for what types of practices an AG could or should prohibit.
  - The core of the provision is the requirement to avoid subjecting individuals to unreasonable privacy risks. The most straightforward way to do this would be to tie the "duty" to the outcome of the risk assessment which is already required. Section 9 could be re-drafted to prohibit a

controller from engaging in a data processing activity that, after the required risk assessment, is determined to present a material risk of harm to an individual that cannot be mitigated without first obtaining the individual's specific and informed consent to that processing activity.

- **Harmonization with existing privacy laws:** It is important that any new privacy legislation align with and haromonize with existing privacy laws, particularly the GDPR which has significantly influenced privacy laws around the world. This is particularly true for definitions of key terms. Unless there is a specific reason to deviate, IA recommends adopting existing definitions for terms including, but not limited to, "controller," "de-identified," "personal data," and "profiling." Other definitions should also be reviewed to determine how closely they align with the prevailing global standards (GDPR, APEC Cross-Border Privacy Rules) or existing U.S. federal or state laws.
    - **Controller:** IA appreciates that the latest draft now matches the GDPR definition of "controller."
    - **Deidentified:** Deidentification has been a defined process with specific requirements for many years. The prevailing definition for "deidentification" comes from the Federal Trade Commission 2012 report "Protecting Consumer Privacy in an Era of Rapid Change" which identifies the requirements for deidentification, and thus not being treated as "personal data," as: "(1) a given data set is not reasonably identifiable, (2) the company publicly commits not to re-identify it, and (3) the company requires any downstream users of the data to keep it in de-identified form." (FTC Report, p. 22).
    - **Personal Data:** IA appreciates the work has been in the definitions section that clarify the term "personal data." IA supports a definition that focuses on the reasonable capability of data being linked to a specific person. As noted during the April 14 call, including concepts related to devices and households in the definition of "personal data" and "data subjects" raises difficult issues. The core part of existing legal definitions of personally identifiable information or data focus on the link, or reasonable capability of being linked, to a specific natural person. (*See* GDPR, Article 4(1); Cal. Civ. Code § 1798.140(o)(1)). This type of functional definition avoids the pitfalls related to "households" and "devices" as well as the potential for becoming out of date as new data points emerge. It would similarly avoid issues from including "probabilistic inferences" in the definition. Each of these raise technical and practical concerns for access, deletion, correction and portability of personal data. IA recommends adopting the language used in Washington's S.B. 6281, Section 3(22)(a), which simply defines "personal data" as "any information that is linked or reasonably linkable to an identified or identifiable natural person."
    - **Profiling:** The definition of "profiling" has an exclusion for search, but does not apply if the search is saved for any reason (which would include, presumably, for

the user's own reference in search history). IA recommends adopting the definition of "profiling" used in the GDPR (Article 4(4)).

- **"Custodian:"** IA appreciates and supports the deletion of this term. IA shares the concerns expressed during the April 14 meeting and believes that spelling out both controllers and processors in individual provisions of the draft legislation will benefit the committee during the drafting process. To harmonize with existing frameworks, it is very important that the ULC drafting committee carefully consider which obligations should be applied to controller, which to processors, and which to both entities. (Further comments on the processor role are below).
- **Sensitive data:** The current definition does not include data elements commonly included in existing legislation as sensitive data including: SSN, Drivers license number, account numbers and passwords. The definition should be expanded to include this definition. In addition, "sensitive" includes "biometric" information which is undefined currently. For purposes of this uniform law, a uniform definition would be helpful.

- **Further work is needed to further frame key elements of the draft:** IA would like to highlight a few areas where additional work is needed to provide a complete framework for data protection.
  - **Verified Requests:** The current draft does not clearly require appropriate authentication and verification of the identity of the person seeking to exercise the rights provided by draft. Verification is essential for maintaining the privacy, safety, and security of individuals.
  - **Children and minors:** The existing provisions in the draft need be further refined to ensure that there are distinctions between children and teens; create compatibility with the Child Online Privacy Protection Act ("COPPA"); and determine when it may or may not be appropriate for parents or guardians to exercise privacy rights over the data of the minors for whom they are responsible. IA recommends that COPPA is added to the list of statutory exceptions and that "child" be defined to a natural person "under 13 years of age," and that the term "minor child" be replaced by the newly defined term "child."
  - **Scope of the bill:** The newly added language in subsection 4(4), "subject to section 3 of this Act," should be removed as it creates confusion as to the scope of exceptions contained in section 3. This language would seem to suggest that limitations in section 3 do not apply to rights other than deletion. For example, it suggests a data subject's right to correction is absolute and could be used to force a change to data that is material to a criminal investigation or litigation. In addition to removal of that language, IA requests that the drafting committee expand the scope of the bill as well as the exceptions to the bill's requirements in section 3, subsections (b) & (c), specifically by:
    - Considering expansion of the scope to cover state and local governments;

- More clearly excluding business-business transactions;
- Including contractors in the employment exception in (b)(6);
- Revising (c)(2) to add "threats to physical safety";
- Adding exceptions that are important in the context of a complying with data subject rights and drawn from existing privacy law, as follows: Nothing in the Act shall—
    - require a covered entity to undertake actions that would compromise the privacy, security, or other rights of the personal information of another individual (for example, when exercising rights would give a person access to someone else's information);
    - require disproportionate effort, taking into consideration available technology/are infeasible on technical grounds;
    - require a covered entity to disclose the covered entity's trade secrets or proprietary technology or business insights;
    - require the covered entity to re-identify or otherwise link information that is not already maintained in a manner that would be considered personal information; or
    - violate federal or state law or the rights and freedoms of other individuals, including under the United States Constitution.

- **Risk Assessments:** As drafted the risk assessment obligation is very broad as it covers all processing activities. This will likely cause an unnecessary administrative burden on smaller businesses. Instead, risk assessment, like Data Protection Impact Assessments ("DPIAs") in GDPR, should be limited to higher risk data processing activities. However, unlike GDPR which allows member country DPAs to specify processing activities that require DPIAs, it would promote uniformity across states to set the risk threshold in the proposed uniform law.
- **Opt-out:** The draft allows data subjects to restrict processing of their personal data for targeted advertising. Targeted advertising is defined by reference to "profiling." That definition appears to include any tracking of user behavior both within the controller's network and across other sites. IA agrees that data subjects should be able to opt-out of cross-site tracking, but has concerns about the ability to opt-out of First Party advertising based on user activity within a controller's network. This type of advertising is activity that is reasonably expected by consumers and is important to continued success of ad-supported sites. IA would recommend adopting a definition of targeted advertising that recognizes the distinction between First Party and Third Party advertising.

- **Areas for clarification within the draft:** Within the draft there are some areas where the draft may appear to have overlapping requirements or differing definitions or requirements that appear in tension. Further clarification would be helpful in the following areas:

- **Transparency:** IA recommends the drafting committee further consider how the provisions related to the "Privacy Commitment" interact with the "Duty of Transparency." To reduce the burden on businesses, it is preferable that covered entities only need to prepare one public facing privacy statement. If the committee determines that there is value in having a public-consumer facing privacy statement and separate submission to the Attorney General, it will be helpful to only require the additional information necessary for the Attorney General to perform his/her enforcement role. IA believes there are opportunities to leverage codes of conduct to promote transparency and supports the drafting committee considering safe harbors for adoption of widely accepted codes.
- **Processor role:** The draft requires that controllers instruct processors on the scope of authorized processing activities through a written agreement. There are provisions in the draft that are arguably unnecessary in light of this requirement, and the draft would benefit from clarifying or removing those requirements. For example, the draft makes a processor a covered entity if a controller for whom they process data is known or should be known to be covered by state's law. However, through the required written contract between the controller and the processor, the controller should specify any requirements necessary to satisfy applicable laws related to the processing activity. The controller is in the better position to evaluate its legal obligations in any particular jurisdiction, particularly where those obligations may depend on company confidential information such as the number of consumers served in a particular jurisdiction. Another example where there is potential tension between the contract that governs the controller and processor relationship and the requirements otherwise put on processors in the draft is in the Duty of Loyalty which applies to both. Processors may only engage in the processing activities for the purposes that are allowed by its written agreement with the controller. To the extent a processor is acting for its own purposes, it becomes a controller by determining the means and purposes of processing. The Duty of Loyalty provisions appear to require processors to make determinations about whether the activities they are instructed to undertake by controllers are potentially unfair, deceptive, or abusive. Processors are unlikely to have all of the relevant information necessary to make such a decision, and therefore the responsibility for such decisions should rest with the controller.
- **Publicly Available Information:** In the prior draft, "public available data" was defined narrowly to include only records made public by government entities if used according to any specific conditions on use. (*See* Section 2(12)). However, in Section 3(b)(3), publicly available information was carved out the scope of the bill and was expanded to include "generally accessible or widely-distributed media." The latest draft resolved the issue of two potential definitions of the term, but did so by narrowing the concept. As noted by the drafting committee, this is an important issue that raises First Amendment concerns. IA notes that it does have significant implications for controllers and compliance with the requirements

of the act. For example, the right to correct publicly available information raises significant complexities and First Amendment issues and a controller can face liability for a failure to comply with a request. IA proposes that the definition be revised to state: “Publicly available data” means information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public from widely distributed media, or by the consumer, or by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.