



March 12, 2021

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

Dear Chairman Perlman:

Thank you for the continued opportunity to provide feedback on the proposed Collection and Use of Personally Identifiable Data Act (the “Act”). As you referenced in the Agenda and Issues Memorandum for the imminent March 12–13, 2021 Video Committee Meeting, representatives from our and select other Attorneys General offices met with you in January 2021 to express shared concerns about certain provisions at the core of the Act, including its voluntary consensus standard and enforcement provisions. Given that our concerns remain unaddressed, we cannot support the current draft.

As the chief legal officers in our states and the sole contemplated enforcers under the Act, State Attorneys General stand to play a *critical* role in ensuring its privacy rights. As written, however, the Act undercuts our enforcement authority and fails to adequately protect consumers. We therefore object to the Act as drafted and would further object to the Committee moving towards finalization without addressing our concerns.

We begin by addressing Section 15 of the current draft, which provides that the Attorney General of any adopting state must establish a formal process for stakeholders to request recognition of a voluntary consensus standard. If a standard is recognized by the Attorney General, consistent with the enumerated findings requirements, a controller or processor in compliance with that standard is deemed in compliance with the Act. While we appreciate that the drafters afforded this important role to State Attorneys General, our offices are not in a position to endorse specific standards or establish the associated rulemaking processes.

In addition to being out of step with the role of the Attorneys General, such a requirement would be a resource strain on our offices, not just as to available staffing, but also where outside technical expertise would be required. These resource demands would invariably require that the adoption bill contain a fiscal note or impact statement, the inclusion of which is frequently fatal to passage. Further, we caution that Attorneys General may be hesitant to exercise the discretion afforded to them under this section in recognizing a given standard (“The [Attorney General] *may* recognize a voluntary consensus

standard...”) knowing that doing so may hinder their prosecutorial discretion in future enforcement actions. The Act provides no process by which an Attorney General may rescind or otherwise reconsider recognition of a standard. The result would be that the sought-after benefit of uniform standards would not be realized, rendering this provision unproductive.

Even if there were *informal* support for a specific standard amongst State Attorneys General, whether an entity is in compliance with a particular law or standard remains a highly fact-specific inquiry. This brings us to Section 12 of the Act, which creates a sweeping safe harbor for entities that comply with a recognized voluntary consensus standard. Our data privacy investigations have often revealed that an entity that asserts that it has adopted or complied with a particular standard—and that may even have a third-party issued compliance certification—may nonetheless have substantial shortcomings in its data privacy practices. By tying compliance to a specific standard, the determination of whether an entity is compliant becomes an even more fact-specific inquiry, effectively requiring the Attorneys General to act as auditors.

Similarly, Section 11 grants yet another safe harbor, this time for any controller or processor that complies with a similar privacy protection law that the Attorney General deems “equally or more protective” of data privacy than the Act. While we recognize the desire for consistency across regulatory frameworks, this language appears to require us to review laws in other jurisdictions, weigh their protections, and potentially, defer to those laws in deciding whether to pursue an action. For these reasons, as is consistent with our existing investigatory practices, we strongly believe that compliance with other laws and standards should be treated as important factors in evaluating whether a controller or processor is compliance with the Act (and in turn, whether our offices pursue enforcement action), but not dispositive ones.

Notably, the Act’s framework with respect to voluntary consensus standards and enforcement is inconsistent with existing state privacy laws, as well as privacy bills introduced in other states. Given that a chief goal of the Committee is to ensure interoperability, this is a significant issue. In addition to our overarching concerns, we are concerned with other provisions of the Act, including, but not limited to, the wholesale lack of a right to deletion and the existence of sweeping exemptions that would hamper our ability to enforce the law.

We recognize that these concerns strike at key aspects of the Act and that the Committee has taken great strides to get to this point. We also acknowledge and appreciate the changes that have been made at the suggestion or request of representatives of select Attorneys General, but given our remaining concerns, we view this draft as fundamentally unacceptable. There is much work to be done with respect to data privacy rights, and our offices are committed to achieving the best outcome for consumers. We thank the Committee for its part in developing the conversation on this pivotal subject, but we cannot accept the serious flaws in this draft and urge the Committee to address our concerns before finalizing the model law.

Thank you,



William Tong  
Connecticut Attorney General  
Co-Chair, National Association of Attorneys General  
Internet Safety & Cyber Privacy Committee



Wayne Stenejhem  
North Dakota Attorney General  
Co-Chair, National Association of Attorneys General  
Internet Safety & Cyber Privacy Committee