March 30, 2021

To: Drafting Committee and Observers

From: Harvey Perlman and Jane Bambauer

Re: April Draft–Collection and Use of Personally Identifiable Data Act [Proposed new title: Personal Data Protection Act]

This memo accompanies the draft of the Personal Data Protection Act for consideration by the drafting committee on April 23, 2021. The new title is contingent on Conference approval. It incorporates changes approved at the meeting on March 12-13 and the resolution of issues left open at that meeting. The sections related to the latter are high-lighted and this memo describes the changes that were made.

First, however, I want to outline the path forward. The April 23rd meeting will largely be for members of the drafting committee to approve the draft. Observers are welcome to attend but I would like to limit most of the discussion to committee members. We will address the highlighted sections. If time remains, we will be open for further issues or concerns. In that regard, I am asking commissioners and observers to submit any recommended changes, in legislative language if possible, to me no later than April 15th (now that tax day has been postponed) for distribution. It is unlikely we will be able to consider at our meeting recommendations submitted after that date. I will also resist reconsideration of issues that have been debated previously unless overruled by the drafting committee. The approved draft will be submitted to the Style Committee for distribution to all uniform commissioners. There will be an informal presentation of the act on June 4th from 2:00 to 4:00 p.m. CDT to solicit the views of all commissioners. We may have an opportunity to make minor changes thereafter in preparation for the summer meeting when our act will be presented for its second, and hopefully final, reading.

Highlighted Changes to the Draft Explained

Section 1 (2). The definition of compatible data practice was shortened so as not to duplicate the substantive provisions of Section 7.

Section 1(9) & (15); Section 5. We have taken up the suggestion to define and make use of the new term "maintains." This allows us to limit the act to data that are collected for the purpose of retrieving personal data for individualized treatment and communications, as opposed to data systems like email that happens to collect names or other personal details in its contents without the function or purpose of making individualized assessments.

One of the benefits of incorporating the term "maintains" is that it allowed us to expand the protections and rights related to pseudonymized data. Prior drafts had distinguished pseudonymized data from both "personal data" and "deidentified data," but the legal restrictions and obligations that applied to that middle category of data were ambiguous. With the help of the concept of "maintains," we have redefined "pseudonymized data" so that it is a form of personal data. Like all other personal data, controllers may only use or disclose pseudonymized data for compatible data practices. However, the rights of access and correction apply only to pseudonymized data that is *maintained* with *sensitive data*. Pseudonymized data that is not *maintained* (i.e. data that has direct identifiers removed but is only used for research) is not subject to the requirements of access and correction at all.

Pseudonymized data that is maintained for the purposes of individualized treatment or communications are also exempt from the access and correction requirements if it does not contain any of the categories of personal data that is considered sensitive. These changes expand the protection that is afforded by the act to pseudonymized data, but it also gives industry an incentive to pseudonymize data and to drop sensitive attributes in any context where identities and sensitive traits are not necessary.

Section 8. The earlier section (a) included as an incompatible data practice, a compatible data practice in which the data was not subject to reasonable security measures to prevent unauthorized access. It was suggested that this may be an inadequate and confusing way to import data security requirements into our act. We have omitted the provision.

Section 9; Section 16. The earlier section defined prohibited data practices but limited them to practices undertaken with a particular mental state, i.e., "reasonably", "foreseeably", "recklessly", or "knowingly". It was argued that while the mental state of the actor would be relevant with respect to determining the appropriate penalty, it should not be a required provable element for enforcement. We have removed any mental or knowing requirement from this section and have added a section to Section 16 on enforcement that clarifies that remedies other than injunctive or cease and desist orders require some mental state.

Section 11(a). Concerns have been expressed by the Attorneys General that determining whether another jurisdiction's law is equally or more protective than this act draws on the resources of their offices and increases the fiscal burden of our act. We originally authorized the AG to impose a fee for assessing a voluntary consensus standard for compatibility and we have added a comparable provision here.

Section 11(b). At the request of the committee, we moved the provisions relating to major federal privacy laws from Section 3 (scope) to this section. The committee also voted to require that in order for the federal law to supersede this act, the entity would have to be "in compliance with" that federal law. I earlier circulated my view that this latter requirement would be detrimental to the success of our act with little marginal data protection. Observers representing entities regulated by these federal laws have also filed their objections, observing that compliance with multiple regimes is both costly and confusing. In my earlier email I invited the drafting committee to reconsider. I have heard from two original supporters of the change indicating they would be willing to reconsider. I have not heard from others. Accordingly, exercising the minimal power of the drafters, we have not included the incompliance requirement in this draft. Should the drafting committee continue to support that requirement, we will incorporate the "in compliance with" condition.

In the comment to this section I have emphasized that these exemptions are not entity-wide. Entities that process personal data outside the data regulated by these federal acts would be subject to our act.

Section 16 (e). In response to the Attorneys General concerns regarding the fiscal impact of this act, we have authorized the Attorney General to recover the costs of enforcement of this act when the Attorney General prevails. The newly enacted Virginia data privacy statute provides a broader provision that seems to permit the recovery of enforcement costs regardless of whether the AG prevails.

Section 17. This section tracks language that has been used in other uniform laws. Common law or statutory causes of action for violation of rights of privacy exist in most states. This provides assurance that those private causes of action remain unaffected.