April 21, 2021

To: Drafting Committee and Observers

From: Harvey Perlman and Jane Bambauer

Re: SUPPLEMENTAL MEMO: April Draft: Uniform Personal Data Protection Act

This memorandum accompanies a redline version of the draft for our April meeting. We apologize in advance for how complex the changes may appear in redline form. We have tried to evaluate and respond to comments we received from commissioners and observers that were received prior to April 15th. We have considered them all. We have adopted many. We have rejected some. We received a number of suggestions from the Internet Association after the deadline. We have not had the opportunity to evaluate or respond to them. We intend to do so after our meeting on April 23rd.

In addition to the highlighted (in yellow) provisions which are explained in our earlier memorandum, the following are the significant (in our view) substantive changes in this redline draft.

1. The Executive Committee approved the name change and the designation "uniform" for our act. We are now officially the Uniform Personal Data Protection Act.

2. We have consolidated the definition of "compatible data practice" into the substantive provision of section 7.

3. Employment data. Jane and I have become convinced that we should exempt employee data from our act. You will find our language in Section 3. We have been urged to do so, in part because most of the enactments or proposals contain such exclusions, and in part because employment lawyers have indicated to us that the regulation of employment data has unique complexities that merit separate treatment.

4. There was concern expressed by some about when controllers or processors should be responsible for each other's conduct. Our original draft made collecting controllers responsible for prohibited data practices of third party controllers or processors if they "knew or had reason to know" of the prohibited practices. We did not make processors responsible for the conduct of controllers. The concern was both with the "should have known" standard being too vague and the lack of similar liability for processors who in many instances have more leverage over data uses than controllers. We have made the potential liability go both ways and have eliminated the "should have known" language. We now require the party to be held responsible to know of the other party's conduct and to have a reasonable way to prevent it.

This is not without controversy and both of us are uneasy about making processors responsible for controllers' conduct. The argument in favor is that large processors often dictate the terms of the processing agreements (i.e., hot dog stand signing processing agreement for credit card transactions with Visa). A large processor could insist on authorizing a incompatible data use. The other side is that if such occurred the controller can either refuse to agree (unlikely) or to seek consent from data subjects for the incompatible use. The processor would, of course, be responsible for its own conduct in

processing for an incompatible use. And if the controller agreed to the demand, it would also be responsible under any circumstances.

5. There was concern that the nondiscrimination language in section 5 might be read too broadly to capture corrections to data that would justify a change in service, such as a change that made the data subject ineligible to receive benefits under a loyalty program. We have addressed this concern in a comment to section 5.