JAMES BOPP, JR.
jboppjr@aol.com

THE BOPP LAW FIRM, PC
ATTORNEYS AT LAW

THE NATIONAL BUILDING
1 South Sixth Street
TERRE HAUTE, INDIANA 47807-3510
Telephone 812/232-2434 Facsimile 812/235-3685
www.bopplaw.com

To Harvey Perlman, Chairman CUPID Drafting Committee

From: James Bopp, Jr., ULC Commissioner, Indiana

Date: August 11, 2020

Re: Proposal for a Compromise Draft

Thank you for your memo of August 7, 2020, presenting the question whether the CUPID Committee should make an either/or choice between the Collection and Use of Personally Identifiable Data Act ("CUPID") and the Personal Data Protection and Information System Security Act ("PDPISS"); or, alternatively, create a compromise draft using the best aspects of both laws.

As set forth below, I believe the Committee should create and adopt a compromise between the two bills. I propose that this be accomplished by adopting the framework of PDPISS and expanding its scope to bring it closer to the universal coverage sought by the CUPID. The idea is to create a compromise draft that has a much larger regulatory footprint than the Alternative Draft, while retaining its cost efficiencies, workability and effectiveness.

The Current Committee Draft

CUPID seeks to achieve comprehensive personal data privacy protection, based in part on the California Consumer Privacy Act ("CCPA") and in part on the European Union's General Data Protection Regulation ("GDPR"). It also includes several novel elements not presently found in any existing privacy legislation. Because of its prescriptive framework and high implementation costs, CUPID has failed to gain the support of most industry stakeholders. The exception to this is the large multinational tech companies, who, having invested what they describe as "billions of dollars" in compliance with the California and European regulatory models, have a competitive interest in supporting a legal framework that requires their domestic U.S. competitors and small and medium businesses to incur these costs as well.

Some privacy advocates also support CUPID, primarily the large organizations that supported CCPA. However, CCPA and the Washington Privacy Act, which CUPID is largely based on, have been widely criticized by the majority of privacy advocates, causing the Washington Privacy Act to fail twice to achieve passage, and the failure in other state legislatures of frameworks similar to CCPA. The key issue for advocates is the notice and consent "check-box" approach of the CCPA and GDPR frameworks, which fail to provide actual privacy protection to consumers (CCPA's opt-out rate is less than 1%), and perpetuate control of personal data in the hands of large tech industry platforms.

Another key criticism by privacy advocates is the way the CCPA and GDPR frameworks force businesses to build new "consumer data silos," creating new data security and privacy risks. The CUPID framework has yet to resolve these challenges, nor has it addressed in a satisfactory manner its interface with the state/federal sectoral privacy regime, its rigid and legalistic reliance on the terms of the notice upon collection, and potential conflicts with the First Amendment.

Finally, even from the perspective of someone who believes that an expensive prescriptive universal privacy law is preferable, many of the novel aspects of CUPID remain undeveloped and inchoate. The idea of a duty of loyalty of a data custodian (defined as either a controller or a processor) and of a data privacy commitment ,with its data privacy minimization requirements, are not found in any other existing consumer data protection laws. Clarifying and developing these novel ideas, and securing widespread "buy-in," presents potentially insuperable challenges. In sum, unlike the CCPA or the GDPR, which contain an inner coherence, CUPID still has an unworked out quality to it, making it a poor candidate on which to build a workable data protection framework that can achieve widespread support.

The Alternative Draft

By contrast, the PDPISS framework is based on the Privacy Act, the E-Government Act, and the COPPA, which have been on the books for 45 years, 18 years, and 20 years respectively—laws that have been tested and have passed the test of time. At the same time, because PDPISS is based on these existing sectoral models, the regulatory framework is narrower in scope, at present limiting itself to protecting privacy interests arising out of consumer transactions for a core set of personal data.

The approach used by PDPISS would keep compliance costs low for business, including small and medium sized businesses, while its robust use of the concept of compatibility keeps notice and consent requirements meaningful, avoiding many of the "check-box" tendencies of statutes like the CCPA and the GDPR. PDPISS's two tiered definition of personal information—one designed for the application of individualized fair information practice protections and the other for the management of system wide risks to privacy and security—also provides a useful and effective regulatory framework. And PDPISS creates strong incentives to develop sector specific voluntary consensus standards allowing the requirements of the Alternative Draft, the concept of compatibility, the privacy protections and the information system security requirements, to be tailored to specific sectors and in different contexts, avoiding the over- and under-inclusiveness characteristic of universal privacy laws like the CCPA and the GDPR.

As noted, however, the main criticism of PDPISS is its narrow scope. It provides effective privacy at an affordable price within the area it covers, but fails to address two additional areas of personal data in the data ecosystems in the modern age.

Taking a step back to get a more general overview of the ecosystem of personal information, there appear to be three main groups of personal data collectors that can be subjects of data protection laws: 1) businesses collecting information directly from consumers (the PDPISS's covered entities), 2) third party users of the data collected by the covered entities, and 3) data brokers. On its face PDPISS addresses only category 1 and a comprehensive approach would cover all three.

Proposal for a Compromise Draft

The feedback we have received from serious privacy advocates and other industry stakeholders is that it will be essential for any personal data protection framework to address the third party users in Category 2, and the data brokers in Category 3. To address this need, and to modify PDPISS to impose a comprehensive regulatory footprint, we proposes that PDPISS be expanded to address Category 2 and Category 3.

Regulating Category 2

In order to address Category 2 unequivocally, Section 4 of PDPISS should be modified by adding a new subsection (c), as follows:

> (c) A third party may process personal data collected in connection with a relationship between a covered entity and a consumer, provided the role of the third party is made transparent to the consumer, and the covered entity enters into a written agreement with the third party subjecting the third party to the same requirements regarding the use of personal data as the covered entity.

With this amendment to Section 4, the scope of the PDPISS can be expanded to cover Category 2, third party users of the data collected by the covered entities. The new Section 4(c) would provide that third party users of data collected by covered entities would be required to adhere to the same compatible uses as covered entities, or obtain the appropriate form of consent from the consumer. The covered entity would be responsible for ensuring appropriate transparency and documentation for its sharing of personal data with such third parties.

This approach is similar to the way the HIPAA regulations treat "business associates" and is an effective and well-understood structure to implement. For example, HIPAA business associates can be many types of businesses -- accounting firms, data processing companies, educational firms, labs, billing companies, and so forth. Standard form agreements can be the subject of industry specific voluntary consensus standards reducing the regulatory cost for businesses.

Regulating Category 3

In order to address data brokers in Category 3, PDPISS needs an entirely new section specifically designed to address the privacy risks data brokers create. Such a new section should be based on Cal. Civil Code § 1798.99.80 (which operates in tandem with the CCPA), to require registration of data brokers, as well as the Vermont data broker registration law. 9 V.S.A. § 2430. These two laws carefully avoid infringing the First Amendment by requiring data brokers to register on a public facing website, disclose general information about its data collection activities, and provide information to members of the public about how to go about requesting an opt-out.

The California statute is substantially similar to Vermont's, except that California residents in theory have the right to exercise opt-out rights, to the extent the information collected by the data broker is not publicly available, protected by the Fair Credit Reporting Act, or otherwise exempt under the CCPA. The CCPA's data broker registry is already in place, and the Vermont law, which has been in place for more than a year, has shown it provides a level of transparency and accountability that benefits consumers and avoids conflicts with the First Amendment. Given the relatively low cost of the Vermont and California laws on this issue, expanding PDPISS to include this kind of registration and opt-out for data brokers, would both broaden the footprint of the bill and would still keep compliance costs reasonable.

While many details of this new section will still need to be worked out, the goal would be to focus on establishing a consumer right to opt-out — similar to the "do not call" registry run by the FTC that was upheld in a First Amendment challenge in *Mainstream Marketing Services, Inc., v. Federal Trade Commission*, 358 F.3d 1228 (10th Cir. 2004).

The Compromise Draft

We propose, therefore, a Compromise Draft, based on the Alternative Draft, by amending Section 4 to explicitly expand Section 4's privacy protections to Category 2, third party users, and by adding a new section, similar to the Vermont and California approaches, to extend regulation to Category 3, data brokers.

These changes would address the concerns about the narrow footprint of the original PDPISS framework and about the need to protect the privacy of personal data in the hands of third party users and data brokers and would represent a compromise that would meaningfully address the most significant criticism of the otherwise effective regulatory framework PDPISS provides.