COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT DRAFTING COMMITTEE

December 6, 2020

To: CUPID Commissioners and Observers

From: Harvey Perlman and Jane Bambauer

Re: Focused discussions for December 11, 2020 Meeting

This memorandum clarifies the Commission's options related to five specific issues that have generated disagreement and debate among our observers: (1) Definitional distinctions that the current CUPID Act draft draws between "controllers" and "processors" and the differences in legal obligations as a consequence of those distinctions; (2) Definitional distinctions between "personally identifiable data," "pseudonymized data," and "de-identified data"; (3) Compatible and incompatible uses of "pseudonymized data"; (4) The administrability and practical value of voluntary consensus standard-making procedures; and (5) A limited private right of action against violators.

We received many other valuable comments as well and continue to incorporate those into the draft. For these issues, however, drafting will benefit from further focused deliberation.

1. Covered Entities

The October draft defined two categories of covered entities as follows:

SECTION 2. DEFINITIONS.

(2) "Data controller" means a person that, alone or jointly with others, initially collects personal data from or about an individual.

(3) "Data processor" means a person that has received authorized access to personal data, pseudonymous data, or deidentified data from the controller.

Several commissioners and observers rightly objected that the draft's use of terminology familiar from the GDPR will cause significant confusion since the scope of "controllers" and "processors" under our Act differs from the scope of those groups as governed by European privacy law. Specifically, some firms that would be "controllers" under GDPR would be "processors" under our act. For example, a firm that purchases or receives personal data from another company and subsequently determines how that data is used would be a "controller" in Europe and a "processor" under the draft.

We agree this risks significant confusion. To clarify the design of the CUPID Act, in this memo we will refer to **four** types of data firms:

Data Collectors- these are the firms that initially collect personal data from an individual data subject either through a transaction or an observation. What the draft act had called "data controllers" will now be called "data collectors" in this memo and throughout our discussion.

Third Party Data Users- these are firms that indirectly receive data about a data subject (rather than collecting it directly from the data subject) and also maintain independence over the uses of the data.

Data Agents- these firms receive personal data from a data collector or from a third party data user in order to perform processing of the personal data on behalf of that data collector or third party data user.

Data Brokers—these firms collect personal data from other than the data subject and sell or license the data to others. They do not fit comfortably into either of the above categories because they do not collect data from data subjects nor do they determine its use (except to the extent that the "sale" of the data is considered such a use. If we understand sale to be a form of use, data brokers are a special subset of Third Party Data Users.)

Under the EU's definitions, data agents would be "processors" and all others would be "controllers". The last draft of CUPID, by contrast, treated both third party data users and data agents as "processors."

In considering how the act should treat each of these types of data firms, it is important to consider the fundamental obligations the act seeks to establish within the data industry:

1. The obligation to permit a data subject to access and copy their data.

2. The obligation to permit a data subject to correct their data if it is inaccurate.

3. The obligation to be transparent to the data subject about the nature of collection, redisclosure, use, and security of the data subject's data.

4. The obligation to limit use of the data to compatible uses and to secure the consent of the data subject for incompatible uses.

5. The obligation to avoid prohibited uses of the data.

The act must account for two issues: on which firms are the obligations imposed and which firms bear responsibility for the actions of other firms.

The next draft will avoid confusion in terminology by using the terms “controllers” and “processors” only if their meaning matches the GDPR definition. Nevertheless, the practical consequences of these definitional questions are not nearly as significant as they might appear because **CUPID, as drafted, would require data collectors, third party data users, and data agents to process data only in ways that are compatible with its initial collection.** A third party data user and a data agent, no matter what they are called, will be in violation of the law and subject to enforcement actions if they disclose or use personal data in a manner that is prohibited, and they are also in violation if they use data in an “incompatible” manner without the data subject’s consent. Moreover, any compatible data practices that are used by third party data users or by data agents must be disclosed in the data collector’s privacy policy. Finally, the data collector will have strong incentive to put contracts and other precautions in place in order to ensure that third party data users and data agents use any disclosed personal data only for specific, compatible purposes specified in advance because if a third party data user or data agent engages in a prohibited data practice, or in an incompatible data practice for which consent has not been obtained, legal liability will attach to the third party data user *and* to the initial data collector.

For example, if a data collector sells personal data to an aggregating company, and that company subsequently uses the data in a manner that contradicts the privacy policies published by the data controller, that unconsented incompatible data practice would result in legal liability for the aggregating company and for the data collector.

In this sense, CUPID is slightly *stronger* than the GDPR because the liability of one downstream controller will automatically be shared and attributable to the initial data collector whereas the GDPR will hold the first controller responsible only if it is in some way “responsible” for the event giving rise to liability. (Art. 82 (3).) For this reason, one observer commented that we might consider incorporating into our act a due diligence exception that would allow a data collector to avoid legal risk if a downstream data user unforeseeably misused the personal data.

In contrast to some of the comments we received, we do not believe that structuring CUPID around initial versus downstream collection fails to create “meaningful limitations” on how downstream users handle personal data. To the contrary, the only legal requirements that third party data users and data agents are relieved from are the obligations to respond to individual requests to copy and correct their personal data. This design prevents the Act from creating new data security problems that can emerge if third party data users and data agents, who will usually not have a direct relationship with data subjects, have to provide or correct personal data to somebody claiming to be a particular data subject.

Issues to discuss at the meeting:

Ultimately the issue for the committee is whether the distinctions we draw between actors are the most important distinctions to make and, if so, which types of actors should bear the risk of liability for violations of the act. Two options include:

1. Should the CUPID Act harmonize more with the GDPR by using the "controller" and "processor" distinctions as defined under European law? If so, third party data users will have to allow data subjects to access and correct their data, if verification and authentication is practicable. This will cause some administrative burden and will also create some uncertainty around how courts will interpret reasonable efforts to authenticate requests.

2. If the CUPID Act continues to distinguish between data collectors and others who receive data second-hand, should data agents (those processing data only at the direction of a data collector or third party user) be treated differently from third party data users? For example, consistent with GDPR, should data agents be protected from legal liability based on an incompatible or prohibited use of data if their processing was consistent with the explicit directions of the third party data user or data collector for whom they are processing data?

2. Categories of Data

The October draft defined three categories of data:

SECTION 2. DEFINITIONS.

(7) "Personal data" means information that identifies or describes a particular individual by name or by other direct identifiers such as addresses, recognizable photographs, telephone numbers, and social security numbers. The term does not include pseudonymized data or deidentified data.

(8) "Pseudonymized data" means information that was derived from personal data by removing direct identifiers. A controller or processor can create pseudonymized data by replacing direct identifiers with a unique ID or other code that allows the pseudonymized data

to be converted back to personal data with the use of a decryption key. The term includes information containing Internet protocol addresses or other data related to a particular devices as long as direct identifiers are not included. The term does not include deidentified data.

(4) “Deidentified data” means personal data that has been modified to remove direct identifiers and to use technical safeguards to ensure the data cannot be linked to a specific individual with reasonable certainty by a person who does not have personal knowledge of the relevant circumstances.

The draft also differentiated between different types of personal data by defining “publicly available information” (which can be collected without triggering the legal obligations of the Act) and “sensitive data” (which receives heightened protection).

We received several excellent suggestions for clarifying and better defining publicly available information (especially as it relates to public records) and sensitive data. We look forward to incorporating those in the next draft**.** One of the issues raised is whether publicly available data should be entirely exempt from our act or whether it should at least be subject to the obligation to provide access, correction, and transparency.

For the December meeting, we hope to discuss concerns raised with respect to the definition of personal data, and how to distinguish between it and deidentified data. We received several comments that “personal data” is still too ambiguous because the meaning of a “direct identifier” is context-dependent. We also heard concerns that the definition of deidentified data may be insufficiently well-defined because there is an argument that it is not possible to ensure that data cannot be linked to a specific individual.

We are committed to improving these definitions. The approach the current draft takes is similar to that of GDPR, which also recognizes three distinct levels of identifiability (personal data, pseudonymized data, and anonymous information). Like CUPID , the GDPR uses an objective standard of risk to differentiate anonymous information from personal data. Recital 26 of GDPR states

> “To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into

> consideration the available technology at the time of the processing and technological developments."

However, the GDPR regulations do not clarify whether personal data automatically becomes either pseudonymized or anonymized data, or whether information can have direct identifiers removed but still remain fully protected personal data. The draft CUPID makes clear that data that does not contain a traditional direct identifier would *not* be fully protected personal data. It would be either pseudonymized or deidentified data. The draft act also diverges from GDPR and other privacy laws by explicitly prohibiting the reidentification of personal data that had previously been deidentified. This would create clear legal liability for the actor that misuses properly deidentified data. (*See* Section 9 (d) of the October draft.)

Thus, we have attempted to make the definitions clearer (with the caveat that some concepts, like identifier and "reasonably ensure" are inevitably open to future interpretation).

Modest revision to definitions:

(7) "Personal data" means information that identifies or describes a particular individual by name or by other commonly recognized direct identifiers such as addresses, recognizable photographs, telephone numbers, and social security numbers. The term does not include pseudonymized data or deidentified data.

(4) "Deidentified data" means personal data that has been modified to remove commonly recognized direct identifiers and has undergone a deidentification process that reasonably ensures the data cannot be linked to a specific individual by a person who otherwise does not have personal knowledge of the circumstances in which the data was collected and who does not have special access to the data subject's private information.

(8) "Pseudonymized data" means information that was derived from personal data by removing commonly recognized direct identifiers. A controller or processor can create pseudonymized data by replacing such direct identifiers with a unique ID or other code that allows the pseudonymized data to be converted back to personal data with the use of a decryption key. The term includes information containing Internet protocol addresses or

other data related to a particular devices as long as direct identifiers to a particular data subject are not included. The term does not include deidentified data.

An alternative approach is to define data based on how it is used rather than what it is. Under this approach, personally identifiable data (or "personal data") is that which is used to *recognize and interact with* a distinct data subject at some time after the initial collection of the data. With this approach, the requirements of the act are triggered when and because the data is used to facilitate a new communication or interaction with a data subject. By contrast, if data is used to assess trends or discover insights without reference to individual data subjects, that use falls outside the scope of the act. The concept of deidentification would no longer have to be defined. Instead, the risk that deidentified data might be reidentified by some downstream party would be treated as a data security risk when an actor uses data to recognize and interact with a data subject without authorization.

Issues to discuss at the meeting:

- Should the CUPID Act define personal data based on how it is used rather than the tri-partite classification currently set out in the draft?
- Can the definitions benefit from any further clarification?

3. Processing of pseudonymized data

The last draft allows data collectors and third party data users to pseudonymize personal data and share it with others for behaviorally targeted messaging.

SECTION 2. DEFINITIONS

(14) "Targeted content and advertising" means purely expressive content or advertising displayed to an individual on the basis of profiling.

(15) "Targeted decisional treatment" means differential treatment of, or offers made to, an individual on the basis of profiling.

SECTION 7. COMPATIBLE DATA PRACTICE.

(d) A data controller may use personal data for the purpose of delivering targeted content and advertising to the individual. It may also disclose pseudonymized data to data processors for these purposes. This provision applies only to targeted delivery of expressive content, and does not cover disclosures or uses of personal data or pseudonymous for the purpose of targeted decisional treatment unless the processing is compatible for a different, independent reason.

The draft attempts to distinguish between behaviorally targeted messaging, which is permitted as a compatible data practice, and behaviorally targeted decision-making, which is not. The classic example of the former is the use of website cookies that allow third party companies to collect information about a web user's browsing habits and use the information to sell and place targeted advertising. An example of the latter is the use of pseudonymized data to craft a behaviorally targeted price, to make a hiring decision, or to modify any other term of a transaction.

The purpose of the term "purely expressive content" is to ensure that a firm cannot disguise behaviorally targeted decision-making as a form of content. For example, if an advertiser created a link to one page that sold an item for $10 to one group of people based on pseudonymized data, and created a link to a different page selling the same item for $15 to a different group of people, that use of pseudonymized data would *not* be "purely expressive" because the data is determining not just the persuasive messaging, but the actual terms of sale.

Because the distinction between "targeted content and advertising" and "targeted decisional treatment" is used only once, the next draft will remove these terms from the definitions section. Instead, to clarify, will create a separate section on this particular compatible practice.

Revision

SECTION [ ]. TARGETING ADVERTISING AS COMPATIBLE DATA PRACTICE

(a) It is a compatible data practice for a data controller to use profiling based on personal data for the purpose of delivering advertising and other messaging to data subjects from whom they have collected personal data. A data controller may also disclose pseudonymized data to data processors for the purpose of targeted advertising.

(b) Notwithstanding subsection (a) of this section, personal data or pseudonymized data may not be used to particularize the price or any other element of an individual transaction with the data subject unless the processing is a compatible data practice for an independent reason.

Issues to discuss at the meeting:

- Does this revision sufficiently clarify the use of data for behavioral targeting?

4. Voluntary Consensus Mechanisms

The current draft uses Sections 11-14 to create a process for industries to craft rules that are consistent with the act and that firms can voluntarily opt into following in order to comply with the act.

SECTION 7. COMPATIBLE DATA PRACTICE.

(e) A data controller may process personal data in accordance with the rules of any Voluntary Consent standard that recognized in accordance with Sections 11 through 14 to which the data controller has committed in the privacy policy unless the processing has been found to be incompatible or prohibited by a court of law.

SECTION 11. ADHERENCE TO A RECOGNIZED VOLUNTARY CONSENSUS STANDARD. A data controller or data processor complies with Sections 5 through 9 of this [Act], and any regulations under these sections, by complying with a voluntary consensus standard that has been recognized by the [Attorney General].

SECTION 12. PROCESS FOR VOLUNTARY CONSENSUS STANDARDS BODIES.

(a) The [Attorney General] may recognize a voluntary consensus standard only if the standard is developed by a voluntary consensus standards body through a process that:

(1) achieves general agreement, but not necessarily unanimity, through a consensus process which:

(A) consists of stakeholders representing a diverse range of industry, consumer, and public interests;

(B) gives fair consideration to all comments by stakeholders;

(C) responds to each good faith objection made by stakeholders;

(D) attempts to resolve all good faith objections by all stakeholders;

(E) provides each stakeholder an opportunity to change the stakeholder's vote after reviewing comments received; and

(F) informs all stakeholders of the disposition of each objection and the reasons therefor.

(2) provides stakeholders a reasonable opportunity to contribute their knowledge, talents, and efforts to the development of voluntary consensus standard;

(3) is responsive to the concerns of all stakeholders;

(4) consistently adheres to documented and publicly available policies and procedures that provide adequate notice of meetings and standards development;

(5) includes a right for any stakeholder to file a statement of dissent with the Attorney General; and

(6) includes a right to appeal by any stakeholder that asserts that a voluntary consensus standard was not developed in substantial compliance with this section.

(b) In developing a voluntary consensus standard, the voluntary consensus standards body shall reasonably reconcile the requirements of this [Act] with the requirements of other federal and state laws.

SECTION 13. RECOGNITION OF VOLUNTARY CONSENSUS STANDARDS.

(a) The [Attorney General] may recognize a voluntary consensus standard only if the [Attorney General] finds that the standard:

(1) substantially complies with the requirements of Sections 5 through 9;

(2) is developed by a voluntary consensus standards body through a process that substantially complies with Section 12; and

(3) reasonably reconciles the requirements of this [Act] with the requirements of other applicable federal and state laws;

(b) Not later than 180 days after the filing of the request in a record to recognize a voluntary consensus standard, the [Attorney General] shall in a public record decide whether to grant the request and state the reasons for the decision.

(c) A final decision by the [Attorney General] on a request under subsection (b), or a failure to decide within 180 days of the filing of a request, may be appealed to [the appropriate state court] as provided for in [the state's equivalent of 5 U.S.C. Section 706].

(d) Not later than [180 days after the effective date of this [Act]], the [Attorney General] shall adopt regulations under [the state's administrative procedures act] to establish a procedure for recognition of voluntary consensus standards under this [Act].

(e) A voluntary consensus standard recognized by any member state in an interstate compact under Section 14 shall be deemed recognized under this Section.

(f) The [Attorney General] may recognize a voluntary consensus standard if the [Attorney General] of another state has recognized the standard under a law substantially similar to this [Act].

(g) The General Data Protection Regulation (EU), the California Consumer Privacy Act, and any other substantially similar privacy framework that the [Attorney General] determines to be substantially similar to, or more protective than, this [Act] shall be recognized as a voluntary consensus standard. A firm that voluntarily complies with these laws will be in compliance with this act.

(h) The [Attorney General] may adopt a regulation under [the state's administrative procedures act] to set a fee to be charged any person that makes a request under subsection (b). The fee must reasonably reflect the costs expected to be incurred by the [Attorney General] acting on a request under subsection (b).

SECTION 14. INTERSTATE COMPACT FOR RECOGNITION OF VOLUNTARY CONSENSUS STANDARDS.

(a) Upon certification by the [Attorney General] that a federal law has authorized an interstate compact of states that have enacted a law substantially similar to this [Act] for the recognition of voluntary consensus standards, this state adopts the interstate compact when the [Attorney General] provides notice in a record of the adoption.

(b) Once effective, the interstate compact continues in force and, except as otherwise provided for in subsection (c), remains binding on this state.

(c) A member state of an interstate compact under subsection (a) may withdraw from the compact by repealing subsections (a) and (b) of this section. The withdrawal may not take effect until one year after the effective date of the repeal law and until written notice of the withdrawal has been given by the Governor and [Secretary of State] of the withdrawing state to the Governor and [Secretary of State] of each other member state.

(d) A state withdrawing from the interstate compact under subsection (c) is responsible for all assessments, obligations, and liabilities that extend beyond the effective date of the withdrawal.

(e) An interstate compact is dissolved when the withdrawal of a member state reduces the membership in the compact to fewer than five states. On dissolution, the compact has no further effect, and the affairs of the compact must be concluded and assets distributed in accordance with the provisions of the compact.

Commissioners and observers raised concerns about the practical administrability of the voluntary consensus process. Several raised concerns that without congressional action, states would not automatically adopt the consensus standards approved by other state attorneys general. And without uniform recognition, industries would be less likely to put in the effort to design voluntary consensus standards.

Also, compliance with GDPR and the CCPA should satisfy compliance with CUPID, but is better addressed in its own section since adherence to those laws is voluntary, but not a “consensus standard.”

There was sufficient concern about the Interstate Compact provision that our intent is to remove it from the draft. There also appeared to be some misunderstanding as to whether the act was dependent on voluntary consensus standards to establish the substance of the act or whether it was one way in which firms could achieve certainty for compliance purposes. We will address this concern, in part by reorganizing and slight redrafting of the provisions.

We have modestly revised the draft as follows:

Revisions

SECTION 11. ADHERENCE TO A RECOGNIZED VOLUNTARY CONSENSUS STANDARD.

(a) Data controllers or data processors may initiate a process to develop a voluntary consensus standard for compliance with this [act]. A voluntary consensus standard may:

(1) identify compatible data practices for a particular industry;

(2) develop processes and methods for securing the consent of data subjects for incompatible data practices;

(3) develop common methods for responding to data subject requests for access and correction of their personal data, including mechanisms for authenticating the data subject.

(4) construct a format for a data privacy policy that will provide consistent and fair communication of policies to data subjects.

(5) formulate a set of practices that provide reasonable security to the personal data held by the controller or processor.

(5) develop any other policies or practices that are consistent with this act and may reconcile its requirements with those of other data privacy laws .

(b) A data controller or data processor may submit for recognition a voluntary consensus standard to the Attorney General in accordance with section [ ] of this [act].

(b) A data controller or data processor that adopts and complies with a voluntary consensus standard recognized by the Attorney General pursuant to section [ ] of this [act] shall be deemed to be in compliance with this Act.

SECTION 13. RECOGNITION OF VOLUNTARY CONSENSUS STANDARDS.

(a) The [Attorney General] may recognize a voluntary consensus standard only if the [Attorney General] finds that the standard:

(1) substantially complies with the requirements of this [act];

(2) is developed by a voluntary consensus standards body through a process that substantially complies with Section 12; and

(3) reasonably reconciles the requirements of this [Act] with the requirements of other applicable federal and state laws;

(b) Not later than 180 days after the filing of the request in a record to recognize a voluntary consensus standard, the [Attorney General] shall in a public record decide whether to grant the request and state the reasons for the decision.

(c) A final decision by the [Attorney General] on a request under subsection (b), or a failure to decide within 180 days of the filing of a request, may be appealed to [the appropriate state court] as provided for in [the state's equivalent of 5 U.S.C. Section 706].

(d) Not later than [180 days after the effective date of this [Act]], the [Attorney General] shall adopt regulations under [the state's administrative procedures act] to establish a procedure for recognition of voluntary consensus standards under this [Act].

(f) The [Attorney General] may recognize a voluntary consensus standard if the [Attorney General] of another state has recognized the standard under a law substantially similar to this [Act].

Section _. Voluntary Adherence to Adequate or More Protective Laws

(g) The General Data Protection Regulation (EU), the California Consumer Privacy Act, and any other substantially similar privacy framework that the [Attorney General] determines to be substantially similar to, or more protective than, this [Act] shall be recognized as adequate protection. A firm that voluntarily complies with adequate or more protective laws will be in compliance with this act. .

Issues to discuss at the meeting:

- Does this provide sufficient uniformity across states so that industries are likely to invest in the process of creating voluntary consensus standards?
- Should the act state that the Attorney General ***shall*** recognize a voluntary consensus standard if the AG of another state has recognized the standard under a law substantially similar to this Act ***unless*** the Attorney General files, within 180 days, a justification for the refusal of recognition, creating a default of uniformity?

5. Enforcement

Enforcement of the draft act is divided between the state attorney general and private litigants. For issues of first impression, damages are not available. But willful and well-settled violations of the law are subject to a private right of action for money damages (as well as AG enforcement.)

The current draft contains the following provisions:

SECTION 15. ENFORCEMENT BY [ATTORNEY GENERAL].

(a) An [act or practice] by a person to which this [act] applies is a violation of [the state's consumer protection law] if the act or practice:

(1) substantially fails to comply with this [act]; or

(2) deprives an individual of a right under this [act].

(b) The authority of the [Attorney General] to bring an action to enforce [the state's consumer protection law] includes enforcement of this [act].

(c) The [Attorney General] may adopt rules to implement this [act] under [the state's administrative procedure act].

(d) In adopting rules and in bringing an enforcement action under this section the [Attorney General] shall consider the need to promote predictability for covered entities and uniformity among the states by:

(1) examining and, when appropriate, adopting rules consistent with rules adopted in other states; and

(2) giving deference to any voluntary consensus standards developed consistent with the requirements of this [act].

Legislative Note: *In subsection (a), the state should cite to the state's consumer protection law and should use the term for unfair practice that is used in that law.*

Need another legislative note about the state's administrative procedure act.

SECTION 16. PRIVATE CAUSE OF ACTION.

(a) A person may bring a private action for equitable relief, including an injunction, against a controller or processor that processes the individual's personal data in violation of this [act] and in a manner that would be reasonably likely to cause measurable harm.

(b) A person may bring a private action for damages against a controller, processor, or person that knowingly engages in a prohibited data practice in violation of this [act] in a manner that would reasonably foreseeably cause, or is likely to cause, any of the following:

(1) financial, physical, or reputational injury to a person;

(2) physical or other intrusions upon the solitude or seclusion of a person or a person's private affairs or concerns, where such intrusion would be highly offensive to a reasonable person;

(3) increased risk of subjecting a person to discrimination in violation of any state or federal anti-discrimination law applicable to the covered entity; or

(4) other substantial injury to a person.

(c) At least thirty days prior to filing an action under this section, a written demand for relief, identifying the claimant and reasonably describing the violation of the act relied upon and the injury suffered, shall be mailed or delivered to the covered entity. Any covered entity receiving such a demand for relief that, within thirty days of the mailing or delivery of the demand for relief, makes a written tender of settlement which is rejected by the claimant may, in any subsequent action, file the written tender and an affidavit concerning its rejection.

(d) If the court in any subsequent action finds for the claimant and also finds that the relief tendered by the covered entity was reasonable in relation to the injury claimed by the claimant, the claimant's relief shall be limited to the amount tendered. In all other cases, if the court finds for the claimant, recovery shall be in the amount of actual damages.

(e) If the court finds the violation of this [act] was a willful or knowing violation or that the refusal to grant relief upon demand was made in bad faith with knowledge or reason to know that the act or practice complained of violated this [act], the court may award up to three times the actual damages.

We have clarified the language of Section 15 to improve the likelihood that the CUPID Act will be interpreted and enforced uniformly across jurisdictions (see below.) Subsection (d) of the revised section 15 is modeled after Section 9-526 of the Uniform Commercial Code which attempts to make uniform the filing of security instruments. One question is whether that would work in our context.

The private right of action, however, continues to be a contentious issue. We continue to believe that a private right of action is appropriate. Generally speaking, a private right of action causes injustice only when there is some flaw in the right—some miscalculation in the trade-off of societal interests, or an unacceptable level of uncertainty in the scope of the legal obligations. Because the private right of action in our draft is limited to the knowing commission of a prohibited act, the risk of unfairness and uncertainty are diminished. Thus, we have not crafted a revision of Section 16 at this time.

The committee has three choices with regard to a private cause of action:

1. Adopt the current draft or continue to refine to provide a narrow private right of action for clearly bad behavior.

2. Defer to the current consumer protection laws of the states. Several provide a private cause of action, others do not.

3. Expressly prohibit a private cause of action for violations of this act. Some have urged us to do so.

Revision.

SECTION 15. ENFORCEMENT BY [ATTORNEY GENERAL].

(a) An [act or practice] by a person to which this [act] applies is a violation of [the state's consumer protection law] if the act or practice:

(1) substantially fails to comply with this [act]; or

(2) deprives an individual of a right under this [act].

(b) The authority of the [Attorney General] to bring an action to enforce [the state's consumer protection law] includes enforcement of this [act].

(c) The [Attorney General] may adopt rules to implement this [act] under [the state's administrative procedure act].

(d) In adopting rules and in bringing an enforcement action under this section the [Attorney General] shall consider the need to promote predictability for covered entities and uniformity among the states, so far as is consistent with the purposes, policies, and provisions of this [act], by:

(1) consulting, if appropriate, with the Attorney Generals or other personal data privacy enforcement agencies in other jurisdictions that enact an act substantially similar to this [act];

(2) considering any suggested or model rules or enforcement guidelines promulgated by the National Association of Attorneys General or any successor organization; and

(3) considering the rules and practices of Attorneys General or other personal data privacy enforcement agencies in other jurisdictions.

(4) giving deference to any voluntary consensus standards developed consistent with the requirements of this [act], particularly if such standards have been recognized and accepted by other Attorneys General or other personal data privacy enforcement agencies.

Comment

The challenge in uniform state legislation when agencies are given the power to adopt implementing rules and regulations is to continue to assure a reasonable degree of uniform application and enforcement of the substantive provisions. This is not a unique problem here where the state Attorney General or any other personal data privacy enforcement agency will be required to implement and enforce standards that are, by their nature, flexible so they may be implemented by diverse industries.

What remains uniform by adopting this act is the acknowledgement of the rights of consumers to obtain access to data held about them, to correct inaccurate data, and to be informed of the uses to which their data may be put. The distinction in this act between compatible, incompatible, and prohibited uses of personal data would create a uniform approach to the use of personal data although the very concept of "compatible" use is dependent on the nature of the underlying transaction from which the data is collected.

In order to encourage as much uniformity as possible, the state Attorney General is encouraged by subsection (d) to attempt to harmonize rules and enforcement policies with those in other states that have adopted this act. These provisions are derived from section 9-526 of the Uniform Commercial Code which has been successful in harmonizing the filing rules and technologies for security interests by state filing offices.

Legislative Note: *In subsection (a), the state should cite to the state's consumer protection law and should use the term for unfair practice that is used in that law.*

Issues to discuss at the meeting:

- Do the enforcement provisions achieve deterrence without over-deterring reasonable business practices?

- Does Section 15 provide adequate assurance that the act will be interpreted uniformly across jurisdictions?