3/11/2021

Harvey Perlman, Chair
Jane Bambauer, Reporter
Uniform Law Commission

**Re: Collection and Use of Personally Identifiable Data**

Dear Chairman Perlman and Reporter Bambauer:

The Software & Information Industry Association (SIIA) appreciates the opportunity to provide written comments on the Uniform Law Commission's most recent draft of the Collection and Use of Personally Identifiable Data Act (CUPIDA). SIIA is the leading trade association for the digital content and software industries, and connects more than 700 data, financial information, education technology, specialized content and publishing, and health technology companies. Our members reflect the broad and diverse landscape of the digital information age.

SIIA supports the passage of a comprehensive privacy framework in the United States. We believe that privacy is a fundamental value that is essential to individual autonomy and a functioning democracy. Our members support privacy frameworks that balance this fundamental value with equally important values (like freedom of speech and the free flow of the public domain), and that move away from consent frameworks that overburden consumers without providing meaningful protections. Moreover, new privacy frameworks must protect necessary public policy goals, like the prevention and detection of fraud, and exist in harmony with existing federal and state sectoral privacy laws, including HIPAA, GLBA, FERPA, FCRA, DPPA, and others.

The most recent CUPIDA draft achieves many of these goals. It appropriately excludes publicly available information from the scope of the law, and correctly defines that term to encompass information from both government and private sources. It also makes sound policy calls with respect to exclusions for sectoral privacy laws (particularly with respect to the scope of the exclusion for FCRA) and for other important public policy goals, like fraud prevention and detection, research, and responding to compulsory process requests and public disclosure requirements. Lastly, the current draft makes an important step forward away from overreliance on consent for the benefit of all stakeholders, though we recommend a few changes.

The bulk of our comments focus on textual suggestions that we believe can be made to improve the CUPIDA draft. Notwithstanding these suggestions, we have a significant and overarching concern about whether CUPIDA can achieve its goal of uniformity given the recent passage of the California Privacy Rights Act (and its imitations on amendments) and Virginia's Consumer Data Protection Act. With other states poised to pass privacy frameworks this year, we question whether the time for a uniform approach has passed except by federal legislation with preemption provisions. It is difficult to see how CUPIDA will add anything but more complexity to the growing patchwork, particularly when it makes some regulatory departures from the current state models and allows for potentially multiple voluntary consensus standards.

Moreover, the draft continues to contemplate including a private right of action. As others have commented throughout this process, a private right of action undermines the goal of uniformity. It risks divergent interpretations across state courts, disparate protections for consumers, and abusive litigation tactics that are driven by technical violations and not individual harm. It also disrupts the emerging trend for state comprehensive laws **not** to include private rights of action, with both California and Virginia vesting enforcement authority exclusively in state agencies. For these reasons, we urge the drafting committee to adopt Alternative B in Section 17.[1]

**Rethinking Consent**

The current CUPID draft proposes rethinking the role of consent in data processing by acknowledging that data collectors are entitled to process data for compatible purposes, permitting opt-out consent for incompatible data purposes, and requiring express, voluntary, and signed consent for processing sensitive data for an incompatible purpose. SIIA generally agrees with the intentions here, but we are concerned that Sections 6(a)(4) and 8(a)(1) wrongly limit the ability to process data for incompatible data practices if such practices can be anticipated at the time of collection.

Sections 6(a)(4) and 8(a)(1) provide that a data collector can only process data for an incompatible data purpose if that purpose was disclosed in the privacy policy. While superficially sensible, this limitation ignores that incompatible data practices may not always be known at the time of data collection. Indeed, the commentary itself acknowledges this when it notes that "incompatible data practice[s are] an ***unanticipated*** use of data that is likely to cause neither substantial harm nor substantial benefit to the data subject." (emphasis added). CUPIDA should be revised to address this and ensure that processing can take place for post-collection incompatible data practices assuming that consent is sought and obtained. Not doing so will incentivize businesses to over disclose potential incompatible data practices in order to keep the door open.

[1] We note that Alternative A suffers from an additional flaw with the language intended to confer a cause of action for injunctive relief, which courts could interpret to authorize equitable monetary relief. Here, the FTC Act is instructive. Section 13(b) of the FTC Act is the modern cornerstone of the agency's consumer protection and privacy mission because it authorizes the commission in proper cases to seek injunctive relief. *See,* Section 13(b), second proviso. Although this provision does not reference or contemplate monetary relief, many federal courts interpret it to invoke the full equitable authority of the courts, including the power to order equitable monetary relief. (Note: the validity of this interpretation is currently under review by the Supreme Court in *AMG Capital Management, LLC v. FTC )* The private right of action proposed for CUPIDA could be subject to the same interpretation or at a minimum result in a frontline battle with plaintiff's lawyers over whether it does. If this interpretation were successful, companies would be at risk for abusive lawsuits seeking injunctions, equitable monetary relief, and actual damages.

One way to fix this is to revise CUPIDA to require the collectors to include disclosures of incompatible data practices known at the time of collection in their privacy policies and to permit them to rely on opt-out consent for such processing practices. In contrast, CUPIDA can be revised to scale up the consent standard for incompatible data practices involving sensitive data or those that were not disclosed in the privacy policy at the time of collection. This assures meaningful consent is obtained for any post-collection repurposing of data.

**Clarifying the Definition for Incompatible Data Practices**

CUPIDA proposes defining an "incompatible data practice" to mean "a data practice that is not a compatible data practice or a prohibited data practice." The terms "compatible data practice" and "prohibited data practice" are separately defined. The former means "processing consistent with the ordinary expectations, based on the context of data collection, of data subjects or likely to substantially benefit data subjects". The latter means data processing that is prohibited by Section 9 of CUPIDA, which sets forth harmful bases for processing. The problem that arises from including both in the definition of "incompatible data practice" is that it results in illogical and contradictory results in Sections 4, 6 and 8, which set forth standards for disclosing incompatible data practices in privacy policies and for processing incompatible data practices with consent. But how can a business lawfully disclose and obtain consent (whether opt-out or opt-in) for a prohibited data practice that is subject to a per se ban?

For example, in Section 4(a)(4), CUPIDA proposes that controllers can obtain consent for incompatible data practices. Taken on its own, this means that controllers can circumvent the prohibited data practices ban merely by seeking consent. But then, Section 4(a)(5) separately states that controllers cannot process personal data using a prohibited data practice, which stands in contradiction to the prior provision. To clarify this inconsistency, the CUPIDA should be revised to omit the reference to "prohibited data practice" in the definition for "incompatible data practice."

**Data Security Obligations**

In Section 8(a)(2), CUPIDA converts a compatible data practice into an incompatible data practice if there is a failure to meet data security standards. This is ambiguous.

- Is the intention here to make a compatible data practice a prohibited data practice if data security standards are not met? If so, this is inappropriate given that the prohibited data practices are intended to prevent harm. A business can have a data security failure without an actual intrusion or any reasonable likelihood of harm to an individual. The failure to meet data security standards alone cannot and should not render the processing of all data as unlawful barring some other illegality relating to collection and processing.

- Is the intention to convert a compatible data practice for which consent is not required into an "incompatible data practice" within the meaning of our suggested revision to the definition above? If so, it also is inappropriate. First, it proposes that a company can and should be able to rely on opt-out consent for processing personal data without data security

> safeguards. Second, this presumes that companies know at the time of collection that they do not have compliant data security standards when these standards are constantly evolving and changing depending upon market availability, the nature of the data, the risks to the data, likelihoods of threat and other factors. It simply is an impossible burden to meet while providing no added consumer protections beyond the baseline regulatory standard for deploying reasonable data security procedures.

To remedy this issue, we suggest revising CUPIDA to strike Section 8(a)(2).

**Pseudonymized Data**

We agree with CUPIDA's proposal to define "personal data" to exclude pseudonymized data and deidentified data. We are concerned, however, that CUPIDA then goes on to treat pseudonymized data as subject to specific regulatory provisions despite the exclusion from personal data. For instance, "processor" is defined to mean "a person that receives from a controller authorized access to personal data ***or pseudonymized data*** and processes that data on behalf of the controller." Section 4(b)(2) then prohibits a processor from processing both personal data and pseudonymized data for a purpose other than that requested by the controller. Section 7(c) then addresses controllers disclosing both personal data and pseudonymized data to third-party controllers for targeted advertising. Notably, deidentified data is not addressed in any of these provisions.

The better outcome would be to treat pseudonymized data and deidentified data as equally outside the scope of CUPIDA and not just as outside the scope of the definition for "personal data." If the definitional strictures for pseudonymized data and deidentified data are not met, then it becomes personal data and falls within the scope of the entire framework irrespective of whether the controller and/or processor refers to it as pseudonymized or deidentified. Any concerns about relinking pseudonymized data can be addressed by drafting the definition to prohibit it.

**Privacy Policy Disclosures**

Section 6(a)(6) requires controllers to disclose the federal, state, or international privacy laws or frameworks with which a controller complies. It is unclear why that is a relevant policy disclosure to mandate under the CUPIDA framework. If a controller can segment their business and data practices so that only the CUPIDA framework applies to a particular transaction or interaction, then the other privacy laws that the controller complies with in other instances are irrelevant because they do not govern that transaction or interaction. Even where a controller deploys one privacy policy, this requirement appears to be setting up controllers for technical violations and nuisance suits (if the final draft includes a private right of action). There are many federal, state, and international privacy frameworks that may apply across business models, particularly for larger companies. Not only are many irrelevant to the CUPIDA consumer's experience, but many do not have mandated privacy policy practices and it is inappropriate for CUPIDA to make backdoor requirements otherwise.

**Voluntary Consensus Standards**

SIIA opposes the inclusion of provisions authorizing voluntary consensus standards in state privacy frameworks, including one intending to create uniformity like CUPIDA. While we would be amenable to considering this approach in the federal context, at the state level it will only exacerbate divergences and risk a complicated patchwork.

**Conclusion**

We thank you again for this opportunity to provide you with our comments and for considering our concerns. If you have questions, please contact me at your convenience.

**Dated: March 11, 2021**

Respectfully submitted,

SIIA POLICY

Sara DePaul
Associate General Counsel & Senior Director, Technology Policy
SIIA - The Software & Information Industry Association
202-789-4471 Office / 614-439-4392 Mobile / @saracdepaul Twitter
siia.net/policy