Articles + Publications | March 8, 2021

Uniform State Privacy Law Moves Forward With New Approach

Privacy & Cybersecurity Newsletter

WRITTEN BY

Thomas J. Smedinghoff

Virginia has just enacted a new privacy law, and several other states are considering doing the same, including Minnesota, New York, Oklahoma, and Washington. Yet there is another privacy law being developed that is getting very little attention, but which may ultimately overshadow what is currently under consideration. That is the uniform state privacy law known as the "Collection and Use of Personally Identifiable Data (CUPID) Act" which is being developed by the Uniform Law Commission (ULC).

The CUPID Act is the ULC's response to the privacy compliance nightmare that appears to be developing from the proliferation of state privacy legislation. Once completed, the ULC hopes that this uniform state privacy law will provide a template for all 50 states to use in enacting consistent privacy legislation. Started in late 2019, the CUPID Act appears to be on track for completion in summer 2021.

The CUPID Act has changed significantly since the first draft was released over a year ago (see prior article at https://www.lockelord.com/newsandevents/publications/2020/07/uniform-state-privacy). The current draft of the Act (which was released on March 4, 2021) takes a somewhat unique approach to a number of privacy issues, and in many respects appears to provide an alternative to the approach taken in the GDPR and the CCPA.

Controller Responsibilities and Data Subject Rights

Compared to the GDPR and CCPA, the current draft of the CUPID Act somewhat narrows the responsibilities of controllers that collect data from individual data subjects. Under the current draft, the Act imposes six basic **responsibilities on controllers** – i.e., a duty to:

- provide data subjects with a copy of their personal data upon request;
- correct an inaccuracy in an individual's personal data upon request;
- provide appropriate notice and transparency regarding their data processing practices;
- obtain data subject consent for any processing that would constitute an "incompatible data practice;"
- conduct regular data privacy and security assessments.

Likewise, the draft Act does not provide all of the **data subject rights** included GDPR or CCPA. Most notably, the right to data deletion is not included. Instead, the Act grants data subjects three basic rights – i.e., the right to require controllers to:

- provide data subjects with a copy of their data;
- correct inaccuracies in the data retained; and
- provide redress for any “incompatible” or “prohibited data practices.”

New Approach to Regulation of Processing Practices

The draft CUPID Act regulates the processing practices of a controller with reference to **three new data privacy processing concepts**: (i) “Compatible Data Practices,” which are allowed; (ii) “Incompatible Data Practices,” which are prohibited unless the controller satisfies certain notice and consent requirements at the time of collection; and (iii) “Prohibited Data Practices,” which are not allowed. They may be summarized as follows

Compatible Data Practices: These are practices that involve the processing of personal data that are either (i) consistent with the “ordinary expectations” of data subjecst in the context of the data collection, or (ii) if inconsistent, are likely to substantially benefit the individuals whose data is being processed. Controllers and processors are authorized to engage in Compatible Data Practices without the data subject’s consent.

Incompatible Data Practice: An Incompatible Data Practice is one that is not consistent with typical expectations and is not likely to substantially benefit the individual data subjects. This includes a practice that contradicts the controller’s privacy policy, as well as a failure to provide reasonable data security to protect the personal data. Controllers are prohibited from engaging in Incompatible Data Practices *unless*, at the time the personal data was collected from the consumer, (i) the data subject was given sufficient notice that the personal data might be processed for incompatible purposes, and (ii) the data subject had a reasonable opportunity to withhold consent to that incompatible use. The controller that collected the data is also responsible for incompatible data practices by its processor and by any third party controller to whom it transferred the data.

Prohibited Data Practices: A Prohibited Data Practice is processing of personal data in a manner that reasonably and foreseeably would:

- inflict significant financial, physical, or reputational harm;
- cause the misappropriation of personal data for purposes of identity fraud;
- cause intrusion upon the solitude or seclusion of a person;
- constitute a clear violation of federal or other state law;
- recklessly or knowingly fail to provide reasonable data security measures;
- involve processing without consent data that the controller or processor knows is an incompatible practice, or that a court or the Attorney General has determined to be an incompatible practice;
- recklessly or knowingly cause an increased risk of subjecting a person to discrimination that would violate state or federal law, or
- cause undue risk of harm that cannot be cured effectively by consent.

Safe Harbor for Compliance

The draft CUPID Act also includes two safe harbors for compliance. First, the Act provides a safe harbor for compliance with a similar privacy law in another jurisdiction if the enacting state’s Attorney General determines that such law is as or more protective of data privacy than this Act.

Second, the draft Act introduces a new concept referred to as a “voluntary consensus standard,” and provides a safe harbor for covered businesses that comply with a voluntary consensus standard recognized by the enacting state’s Attorney General.

The Act defines the concept of a voluntary consensus standard, and specifies requirements for recognition of such a standard by the Attorney General. Basically, to be recognized by the Attorney General, a voluntary consensus standard must substantially comply with the key requirements of the Act, be developed by a voluntary consensus standards body through a process specified in the Act, and reasonably reconcile the requirements of the Act with other applicable federal and state laws.

Further Information and Input

With the proliferation of privacy legislation, the project to draft the CUPID Act bears close watching, as the influence of uniform laws drafted by the ULC can be significant. Two of the best-known examples are the Uniform Commercial Code (adopted in all 50 states) and the Uniform Electronic Transactions Act (adopted in 48 states). In this climate, where most states are already looking to address privacy, a uniform law produced by the ULC may offer a well-vetted option.

The ULC drafting committee process is very open and transparent. All of the documents are publicly available, and anyone is allowed to attend and participate in drafting committee meetings. The ULC also encourages the submission of written comments. So far, the project has attracted over 200 observers from a wide variety of industries and consumer groups, and over 30 organizations have submitted written comments.

Information regarding the status of the CUPID Act, as well as the current draft of the Act, submissions by outside groups, and meeting information is available at the ULC website at https://www.uniformlaws.org/home. The Collection and Use of Personally Identifiable Data Drafting Committee page (where all of the documents can be found) is at https://www.uniformlaws.org/projects/committees/drafting.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber