Articles + Publications | October 4, 2021

A Step Toward a Uniform State Privacy Law: The Uniform Personal Data Protection Act

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos | Mark Backofen

This summer, following two years of work toward a model state privacy law, the Uniform Law Commission (ULC) has entered the privacy debate by adopting The Uniform Personal Data Protection Act (the "Uniform Act") by a vote of 52-1, with Maine being the only dissenting vote. The Uniform Act takes a different approach to privacy protection than existing legislation in California, Virginia and Colorado. For example, while it includes a right for a data subject to obtain a copy of his or her personal data and correct inaccurate data contained therein, there is no right to require a company to delete personal data. Some of the other unique features of the Uniform Act are as follows:

Categories of Use

The approach in the Uniform Act creates three categorizes of data practices, and regulates the use of personal data based on the type of data practice involved.

- Compatible Data Practices: Generally, practices that are (i) consistent with the consumer's expectation based on the particular transaction, or (ii) likely to benefit the consumer. Notably, the use of personal data, or even its disclosure to a third party if it is pseudonymized, for the purpose of targeted advertising is considered a compatible data practice. A controller is free to use personal data for compatible data practices, without any need to obtain the individual's consent or provide a right to opt-out of such use.
- Incompatible Data Practices: Unanticipated practices that neither benefit nor harm the individual. Practices that would otherwise be considered compatible data practices are deemed incompatible data practices if they are not adequately disclosed in the applicable privacy policy. Personal data can be used for incompatible data practices only if the practice is adequately disclosed at the time personal data is collected. If sensitive data is involved, the entity will also need the individual's express signed consent for such incompatible data practice, while if no sensitive data is involved, an opportunity to opt- out of the incompatible data practice is sufficient. For this purpose, "sensitive data" is defined to mean personal data that reveals information that would typically be considered sensitive to an individual, including racial or ethnic origin, religious belief, gender, sexual orientation, citizenship or immigration status; credentials sufficient to access an account remotely; financial account number; Social Security number or other government issued ID number; geolocation in real time; criminal record; income; health condition information; genetic sequencing information; and information about a minor under 13 years old. An entity can even require an individual's consent to an incompatible data practice as a condition for getting a discount or even being able to access to goods or services.
- Prohibited Data Practices: Generally, practices that are likely to cause substantial harm, including financial, physical, or reputational harm, embarrassment or harassment, to the individual. It also includes the failure to provide reasonable data-security measure, the use of incompatible data practices without the required consent, and the re-identification of pseudonymized or de-identified data except in limited circumstances. As the name suggests, prohibited data practices are not allowed to be carried out under any circumstances.

Scope of the Act

Unlike most existing privacy laws, application of the Uniform Act is not expressly limited to larger entities, as it applies, at least in part, to any person (defined broadly to include individuals and entities) that maintains personal data and conducts business in the particular state or provides services purposefully directed to its residents. To avoid undue burdens on smaller businesses, however, the Uniform Act provides thresholds below which a person can avoid most of its restrictions. Specifically, the Uniform Act exempts persons that do not: (1) maintain more than [50,000] records regarding individuals from that state; (2) earn more than [50] percentage of gross annual revenue from maintaining personal information as a controller or processor; (3) act as processor for a controller the processor knows to meet the thresholds in (1) or (2); or (4) maintain personal data, unless it processes the data solely using compatible data practices. Note that the amounts of the records and revenue thresholds are bracketed, inviting states to adopt their own thresholds. Compatible data practice is defined to mean processing consistent with the ordinary expectations of data subjects or likely to benefit data subjects substantially, considering listed factors to be considered. Therefore, even persons exempt from the Uniform Act because they are under the thresholds must limit their data processing activities to compatible business practices, or the entire Uniform Act applies.

Similar to other privacy laws, the Uniform Act covers a broad range of information under the definition of personal data. Any record (tangible, electronic or other medium) that identifies or describes a data subject by a direct identifier, and pseudonymized data, but not deidentified data. Deidentified data means personal data that lacks direct identifiers, reasonably ensuring that the record cannot be identified to a data subject without personal knowledge or special access to the data subject's information. There are exemptions for certain data, such as publicly available information, and information processed in the course of employment or an application for employment.

Requirements of the Uniform Act

The Uniform Act imposes requirements on controllers and processors. A controller is a person that determines the purposes and means of processing; a processor is a person that processes personal data on behalf of a controller.

Controllers are required to provide rights to copy and correct personal data, and disclosures about maintenance of personal data and processing practices. Consent is required for processing that is an incompatible data practice, defined as neither a compatible nor prohibited data practice, or inconsistent with the person's privacy policy, which is required under the Uniform Act. Prohibited data practices, which are prohibited, are defined to mean processing: (i) likely to subject a data subject to specific and significant harm (as elaborated in Section 9(a)); (ii) in violation of other law; (iii) without reasonable security measures; or (iv) without consent required for an incompatible data practice. Controllers much also conduct privacy and security risk assessments, and (v) provide redress for incompatible or prohibited data practices.

The Uniform Act requires processors to: (i) provide the controller with access to the personal data; (ii) correct inaccuracies on request of the controller; (iii) limit processing to the purpose requested by the controller; (iv) conduct and maintain privacy and security risk assessments; and (iv) provide redress for incompatible or prohibited data practices.

Deemed Compliance

Compliance with specified federal privacy laws, including the Health Insurance Portability and Accountability Act, Fair Credit Reporting Act, and Gramm-Leach-Bliley Act (among others) can be deemed compliance with the Uniform Act, but only in connection with processing that is the subject of those statutes. Thus, it does not provide a blanket exemption for these regulated entities. For example, a bank that processes information in a manner not subject to Gramm- Leach-Bliley would still be subject to and have to comply with the Uniform Act with respect to that processing.

The Uniform Act also allows by compliance with (i) a comparable privacy law of another jurisdiction (such as the CCPA or GDPR) or (ii) a voluntary consensus standard to be considered sufficient to comply with this Uniform Act. These methods of deemed compliance apply only if the state attorney general has determined that the comparable law is equally or more protective that the Uniform Act, or has specifically approved the voluntary consensus standard.

Enforcement

Enforcement, and particularly whether to include a private right of action, was probably the most hotly contested provision during the development of the Uniform Act. The final Uniform Act attempts to dodge the issue by providing for enforcement through the state's existing consumer protection act. Some states have a consumer protection act that provides for a private cause of action and others do not. The Uniform Act also contains optional language a state can use to preclude a private cause of action under the Uniform Act even if its consumer protection act provides one. As a result, the fight regarding whether to include a private cause of action will now move to the various state legislatures that consider enacting the Uniform Act.

The ULC intends that the Uniform Personal Data Protection Act will promote consistency by providing a template for the states to use in enacting their own privacy laws. The ULC plans to start promoting adoption by the states starting in Jan. 2022, when many state legislatures begin the new legislative session. It remains to be seen whether the ULC is successful in getting the 47 states that do not currently have a comprehensive privacy legislation to enact the Uniform Act, and how much its unique concepts regarding privacy protections will influence future privacy legislation.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber