
Draft of Proposed Model Law on Privacy: 2021 As Approved Act: The Uniform Personal Data Protection Act

*Wilhelmina Randtke
Fact Checker, Dotdash*

Introduction

In July 2021, the Uniform Law Commission (ULC) approved and recommended for enactment in all states the Uniform Personal Data Protection Act (UPDPA).¹ This was formerly discussed at ULC as the Collection and Use of Personally Identifiable Data Act (CUPID Act).² The UPDPA, when finalized, will serve as a model law which state legislatures can introduce and adopt governing how corporations can use information about individuals. At this time, the UPDPA is final as far as substance goes. It is still subject to stylistic revisions³ and should be finalized by January 2022. At that time, the UPDPA will be ready to be introduced to state legislatures for potential adoption. In light of current internet trends for web companies to gather large amounts of information on users, states have begun regulating privacy, and the UPDPA is an attempt to facilitate standardization across states.

Recent laws governing corporate use of personal data on individuals in the United States (U.S.)

The European Union's General Data Protection Regulation (GDPR) became effective May 25, 2018.⁴ This law doesn't apply in the U.S., per se. However, it applies to companies which control or process information on European Union residents, even if they are based in the U.S. and are physically located entirely out of the EU. In 2018, many U.S. based corporations implemented the GDPR with items such as a posted disclosure or privacy notice. For example, many U.S. universities implemented GDPR through posted privacy statements, and many commercial and news websites now pop up GDPR disclosures or consents. This is motivated by a desire for websites to remain accessible to a European audience.

Recently passed state privacy laws include:

- The California Privacy Rights Act, passed in 2018, took effect in 2020⁵
- The Virginia Consumer Data Protection Act, passed in March 2021, takes effect in 2023⁶

In March 2021, proposed federal legislation was introduced in Congress, the Information Transparency & Personal Data Control Act.⁷ That's proposed, not passed.

At a high level, the proposed federal law and the UPDPA are less restrictive than are the recently passed state laws. Specifically, the UPDPA does not provide a private cause of action for individuals to enforce it, but rather provides for enforcement by each state's Attorney General for violations. And the UPDPA does not include a right for individuals to have information about them deleted. A possible result of the UPDPA is for faster, more standardized regulation at the state level but for laws that do pass going forward to be less restrictive than would have been had the California law been the most prominent model to follow.

Recent activities at the ULC

For the past 2 years, the ULC's Collection and Use of Personally Identifiable Data Committee met with the goal of finalizing a model law for personal data protection. Committee documents and notes can be found at <https://www.uniformlaws.org/committees/community-home/librarydocuments?LibraryKey=a9e3ffe6-ff68-41fd-add5-031156ee85e5&CommunityKey=9aad6d7-0020-4df2-821d-19aa34084532>. Starting in May 2020, the committee released a tentative first draft and since has accepted comments and released several revised drafts. In July 2021, at its annual meeting, the ULC approved the UPDPA. The July 2021 document is essentially almost final. The text of

the document states, “The following text is subject to revision by the Committee on Style of the National Conference of Commissioners on Uniform State Laws.”⁸

Overview of the UPDPA

The UPDPA is 21 pages long, double spaced, so it is a quick read. The full text is at <https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=009e3927-eafa-3851-1c02-3a05f5891947&forceDialog=0>.

Who is regulated by the UPDPA:

- Applies to an entity doing business in the state and when any of the following are met:
 - maintains personal data about more than 50,000 residents of the state, excluding personal data used solely to process payments⁹
 - earns more than half its revenue by maintaining personal data on individuals¹⁰
 - is a processor acting on behalf of a covered entity under either of the previous two provisions¹¹
 - maintains personal data, unless it processes all personal data using compatible data practices (compatible data practices is defined within the UPDPA)¹²
- “Personal data” does not include deidentified data, so activities involving deidentified data aren't regulated.¹³
- Does not apply to state government entities.¹⁴
- Does not apply to personal data that is publicly available, part of approved human subjects research, processed or disclosed by court order or other legal requirement, public record, or part of the employment application process.¹⁵

Rights under UPDPA:

- Individuals can: Get a copy of records on them and have information about them corrected. Covered entities are required to provide the records and make corrections on request.¹⁶
- Covered entities are supposed to get consent for certain practices (“incompatible data practices” under the UPDPA), not engage in certain practices (“prohibited data practices” under the UPDPA), maintain privacy and security practices, and post a privacy policy describing how data will be used.¹⁷
- Enforcement is through the Attorney General.¹⁸ There is no private cause of action to enforce these rights.

The UPDPA breaks down whether or not consent is required based on how personal data will be used. Different consent levels are required for 3 types of data:

- “Compatible data practices” don't require consent from individuals whose personal data is used. Compatible data practices include: when the subject knows or participates in providing personal data; when the covered entity has to collect the personal data to meet a legal obligation; when the personal data meets a managerial, personnel, administrative, or operational need; is needed to better detect or address fraud; and a catch all for any other purpose determined to be a compatible data practice.¹⁹ The use must be not be incompatible with the privacy policy required by the UPDPA.²⁰
- “Incompatible data practices” require the subjects signed written consent.²¹ Incompatible data practices include any activity that isn't a compatible data practice nor a prohibited data practice.²² The subject's consent to an incompatible data practice can be required in order to access goods or services.²³

“Prohibited data practices” are prohibited. These include: practices likely to cause specific and significant harm, including financial, physical, or reputational harm, and harassment; practices likely to lead to identity theft; practices that violate discrimination laws; and failure to provide security measures.²⁴ Reidentification of deidentified data is also prohibited.²⁵

- 1 Uniform Law Commission, Collection and Use of Personally Identifiable Data Committee, 2021 As Approved Act: Uniform Personal Data Protection Act (July 7, 2021), available at <https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=009e3927-eafa-3851-1c02-3a05f5891947&forceDialog=0> [hereinafter UPDPA].
- 2 Uniform Law Commission, Collection and Use of Personally Identifiable Data Committee, Tentative First Read Draft and Issues Memorandum (May 20, 2020), available at <https://www.uniformlaws.org/viewdocument/tentative-first-read-draft-and-issu?CommunityKey=9aad6d7-0020-4df2-821d-19aa34084532&tab=librarydocuments> .
- 3 UPDPA, at 1.
- 4 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016, O.J. L 119/36.
- 5 Gilad Edelman, California’s Privacy Law Goes Into Effect Today. Now What?, Wired, Jan. 1, 2020, available at <https://www.wired.com/story/ccpa-guide-california-privacy-law-takes-effect/>.
- 6 Kate Andrews, UPDATED: Va. becomes 2nd state with consumer data protection law, Virginia Business (March 1, 2021), available at <https://www.virginiabusiness.com/article/va-set-to-become-2nd-state-with-consumer-data-protection-law/>.
- 7 Information Transparency & Personal Data Control Act, H.R.1816, 117 Congress (2021), available at <https://www.congress.gov/bill/117th-congress/house-bill/1816/text>.
- 8 UPDPA, at 1.
- 9 Id. section (3)(a)(1).
- 10 Id. section (3)(a)(2).
- 11 Id. section (3)(a)(3).
- 12 Id. section (3)(a)(4).
- 13 Id. section (2)(10).
- 14 Id. section (3)(b).
- 15 Id. section (3)(c).
- 16 Id. section (4)(a)(1,2); UPDPA, section (5).
- 17 Id. section (4)(a); UPDPA, section (6); UPDPA, section (10).
- 18 Id. section (16).
- 19 Id. section (7)(a, b).
- 20 Id. section (8)(a)(2).
- 21 Id. section (8)(c).
- 22 Id. section (8)(a)(1).
- 23 Id. section (8)(d).
- 24 Id. section (9)(a).
- 25 Id. section (9)(b).