Armstrong Teasdale

March 11, 2022 • Advisory • www.atllp.com

UTAH JOINS THE RANKS OF OTHER EARLY ADOPTERS OF NEW DATA PRIVACY REGIMES

PEOPLE

F. Scott Galt, CIPP/E

Casey E. Waughn, CIPP/US

SERVICES AND INDUSTRIES

Data Innovation, Security and Privacy

The data privacy world continues to undergo uncertainty when it comes to the data privacy regulatory landscape. For example, the newly formed California agency responsible for creating California Privacy Rights Act (CPRA) regulations recently announced that it will miss the July 1 deadline, pushing the regulations back until Q3 or Q4 ahead of the critical January 2023 effective date.

Adding to this uncertainty are a myriad of states that are revisiting data privacy legislation in 2022. In fact, Utah's legislature recently passed the Utah Consumer Privacy Act (UCPA), becoming the fourth and most recent state to enact sweeping data privacy legislation. The Governor has 20 days from the date of receipt to act on the legislation, and if he does not sign or veto the legislation within this period, it will become law. While Utah's law has vestiges of Colorado's, Virginia's and California's data privacy statutes, there are a few distinct differences.

SIMILARITIES BETWEEN UCPA AND EXISTING REGIMES

Organizations required to comply with the UCPA can take some comfort in knowing much of it is borrowed from existing regulations. For example, the rights to access, review and request deletion of data are similar to other legislative schemes. Like the CCPA, Virginia's Consumer Data Protection Act (CDPA) and the European Union's General Data Protection Regulation (GDPR), companies are also required to enter into written agreements with third parties, vendors and service providers that process data on their behalf.

The UCPA's consumer notice requirements are also reminiscent of existing privacy frameworks. Under the UCPA, data controllers must clearly disclose the categories of data being collected, the purpose for which the personal data is being collected, how collected data will be shared, and with whom it will be shared. They also must provide a mechanism for consumers to opt out of the sale of their data. Controllers must respond to a consumer's request within 45 days.

Finally, like other existing regulations, the UCPA does not contain a private right of action—instead, the attorney general's office is the sole enforcer and is responsible for notifying organizations of deficiencies. The UCPA allows for a

30-day cure period for the organization to cure the deficiency, after which point an enforcement action can be brought.

DIFFERENCES BETWEEN UCPA AND EXISTING REGULATIONS

While the jurisdictional scope of the legislation generally tracks the scope requirements from the CCPA in that it only applies to business with a gross annual revenue of $25 million, it differs from the CCPA (and other privacy frameworks) in that the company **must also** process the data of 100,000 individuals or derive more than 50% of its revenue from the sale of customer data. In other words, the UCPA requires two of three threshold criteria be met in order for the organization to be subject to the UCPA, rather than just one criterion, which is the case under the CCPA/CPRA and other state laws. This may make the initial determination of whether the organization must comply with the UCPA a longer analysis than under other states' regimes, because the organization may wish to more closely analyze whether it meets the threshold requirements and is required to comply with the law.

Another significant difference from other privacy legislation is Utah's attempt to allow the law to be changed outside of action by the state legislature. The provision allows the Utah Attorney General's office to suggest changes to the legislation via an "enforcement assessment" which is due July 1, 2025. Proponents of the "enforcement assessment" argue that this will give the Attorney General's office "an unusual opportunity to study how the law works and give feedback on what this law got right, and what we may need to fix."

SUMMARY OF CURRENT STATE LEGISLATION

The table below contains an overview of some of the key differences and similarities between Colorado's, Virginia's and California's data privacy regimes:

	Utah (UCPA)	**Colorado (CPA)**	**California (CPRA)**
Effective Date	December 31, 2023	July 2023	January 2023 with a one-year compliance lookback
Companies Subject to the Law	Companies that meet the following criteria: -gross annual	Companies that meet either of the following: - collect and store the personal data of more than 100,000 consumers; or	Companies that meet any of the following: - gross annual revenue of more than $25 million; - annually buy, sell or share for cross-context

	revenue of more than $25 million; **and** -control or process personal data of 100,000 or more consumer during a calendar year; or derive over 50% of their gross revenue from the sale of personal data and control or process personal data of 25,000 or more consumers Nonprofit entities and institutions of higher education	- derive revenue from the sale of personal data of at least 25,000 consumers Nonprofit entities that meet the above thresholds are subject to the requirements.	behavioral advertising the personal information of 100,000 or more consumers or households; or - derive more than 50% of revenue from selling or sharing for cross-context behavioral advertising personal information Nonprofit entities are exempt.

	are exempt.		
Special Requirements for Sensitive Data?	Yes	Yes	Yes
Consumer Opt-Out Rights?	Yes – on a website-by-website basis	Yes – compliance with a universal opt-out through a global privacy control browser setting required by July 2024	Yes – on a website-by-website basis
Purpose/Processing Limitations	Yes	Yes	Yes
Requires a Risk Assessment or Data Protection Assessment?	No	Yes – for certain processing activities	Yes – for certain processing activities
Special Requirements for Youth Data?	Yes – collection restrictions for children under 13	No	Yes – processing restrictions for children under 16

AT's Data Innovation, Privacy and Security practice has vast experience navigating all aspects of the complex data privacy regulatory scheme and regularly counsels clients – whether business-to-business, direct-to-consumer, e-commerce or anything in between – across a variety of sectors on data privacy obligations. For more information specific to your business needs, please contact one of the authors or your regular AT attorney.

Armstrong Teasdale