How the Utah Consumer Privacy Act Stacks Up Against Other State Privacy Laws

Aaron J. Burstein, Laura Riposo VanDruff, Paul L. Singer

March 17, 2022

As companies wait to see whether the Utah Consumer Privacy Act (UCPA) becomes the fourth comprehensive state privacy law, we are providing an overview of some of the Act's key provisions – and how they depart from comprehensive privacy laws in California, Colorado, and Virginia.

Utah's Senate unanimously passed the UCPA on February 25. The House – also through a unanimous vote – followed on March 2. The Legislature sent the UCPA to Governor Spencer Cox on March 15. Because the Legislature adjourned on March 4, Governor Cox has 20 days from the date of adjournment – March 24 – to sign or veto the Act. If Governor Cox takes no action, the UCPA will become law, with an effective date of December 31, 2023.

In broad strokes, the UCPA is similar to the Virginia Consumer Data Protection Act (VCDPA) and Colorado Privacy Act (CPA). And, like the laws in Colorado and Virginia, the UCPA borrows some concepts from the CCPA – including a version of the right to opt out of the "sale" of personal data.

However, the UCPA pares back important features of all three of these laws. Some of the significant changes include:

- **Applicability.** The UCPA's applicability is narrower than the three other comprehensive state privacy laws. The UCPA applies only to controllers or processors that (1) do business in the state (or target Utah residents with products or services); (2) earn at least $25 million in revenue; **and** (3) either: (a) control or process personal data of 100,000 or more consumers in a calendar year; or (b) derive more than 50 percent of gross revenue from selling personal data **and** control or process data of 25,000 or more consumers. By contrast, the $25 million revenue threshold is an independent basis for the CCPA to apply to a business; and neither the CPA nor VCDPA includes a revenue-based exemption.

- **Exemptions.** In addition to exempting personal data that is subject to sector-specific privacy laws and regulations, such as HIPAA, the Gramm-Leach-Bliley Act, and the Fair Credit Reporting Act, the UCPA provides that the Act does not apply to certain entities, including a tribes, institutions of higher education, and nonprofit corporations.

- **Sale and Targeted Advertising Opt-Out Rights.** Although the UCPA requires controllers to provide consumers with the ability to opt out of sale and targeted advertising, the Act does not

provide a right to opt out of profiling (or otherwise address profiling). Like the VCDPA, the UCPA restricts the definition of "sale" to "the exchange of personal data for ***monetary*** consideration by a controller to a third party." This definition does not include "other valuable consideration," found in the definitions of "sale" under the CCPA and CPA.

- **Opt-Out Consent to Process Most Sensitive Data.** The UCPA does not require opt-in consent to process most sensitive data, unless the data "concern[s] a known child," unlike the opt-in requirements of the CPA and VCDPA. Instead, the UCPA requires controllers to "present[] the consumer with clear notice and an opportunity to opt out" of sensitive data processing.
- **Other Consumer Rights.** The UCPA provides consumers the right to confirm processing and to delete personal data they provided to a controller. Consumers also have the right to obtain a portable copy of personal data that the consumer "previously ***provided to*** the controller." This "provided to" language follows the VCDPA's access and portability right and contrasts with obligations to provide personal data "concerning" (CPA) or "about" (CCPA) a consumer. The UCPA does not provide a right of correction or accuracy.
- **Enforcement and Regulation.** The UCPA does not include a private cause of action, nor does it authorize the Attorney General or other state official or agency to issue regulations. The Division of Consumer Protection, in the Utah Department of Commerce, investigates potential violations and can refer an action to the Utah Attorney General for enforcement. The Attorney General can recover actual damages for consumers and a penalty of up to $7,500 per violation, but only after a 30 day notice and right to cure period.

From a preparation and compliance standpoint, the UCPA – if it becomes law – might not be a game-changer for companies that have built their privacy programs around California's requirements. The Kelley Drye team will explore some of the details of all four state laws – as well as compliance strategy considerations – during a webinar on March 24 beginning at 4:00 pm EDT. In the meantime, we will keep a close eye on developments in Utah and elsewhere.

Colorado Privacy Act (CPA)	**Virginia Consumer Data Protection Act (VCDPA)**	**California Consumer Privacy Act (CCPA as amended by CPRA)**	**Utah Consumer Privacy Act (UCPA)**
Applies to a controller that (1) conducts business in CO or targets products or services targeted to CO residents and (2) meets either of these	Applies to a person that (1) conducts business in VA or target products or services targeted to VA residents; and	A "business" (1) conducts business in CA and collects personal information of CA residents; and (2) (a) has $25 million or more in annual	A controller or processor that (1) conducts business in Utah or targets products or services to UT residents; (2) has $25 million or more in annual

Thresholds to Applicability	thresholds: (a) controls or processes personal data of at least 100,000 consumers in a calendar year; or (b) derives revenue or receives a discount on the price of goods or service from selling personal data or controls personal data of at least 25,000 consumers	(2) meets either of these thresholds: (a) controls or processes personal data of at least 100,000 consumers; or (b) controls or processes personal data of at least 25,000 consumers and derives over 50% of gross revenue from the sale of personal data.	revenue for preceding calendar year as of Jan. 1 of calendar year; (b) annually buys, sells, or shares personal data of more than 100,000 consumers or households; or (c) earns more than 50% of its annual revenue from selling or sharing consumer personal information.	revenue; and (3) satisfies one of these thresholds: (a) during a calendar year, controls or processes personal data of 100,000 or more consumers, or; (b) derives over 50% of gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers.
Opt-in Consent	Opt-in consent required to process sensitive data	Opt-in consent required to process sensitive data	Opt-in consent required to sell or “share” personal information of minors under age 16	Not required for sensitive data (unless the data concerns a known child, and parental consent is required under COPPA)
Opt-Out	Required for targeted advertising, sales, and profiling for legal or similarly significant effects	Required for targeted advertising, sales, and profiling for legal or similarly significant effects	Required for profiling, cross-contextual advertising, and sale; right to limit use and disclosure of sensitive personal information	Required for targeted advertising and sales
	Access,	Access,		

Other Consumer Rights	Portability, Deletion, Correction,	Portability, Deletion, Correction	Access, Deletion, Correction, Portability	Access, Portability, and Deletion
Authorized Agents	Permitted for opt-out requests	N/A	Permitted for all consumer rights requests	N/A
Appeals	Must create process for consumers to appeal refusal to act on consumer rights	Must create process for consumers to appeal refusal to act on consumer rights	N/A	N/A
Private Right of Action	No	No	Yes, for security breaches involving certain types of sensitive personal information	No
Cure Period	60 days until provision expires on Jan. 1, 2025	30 days	30-day cure period is repealed as of Jan. 1, 2023	30 days
Data Protection Assessments	Required for targeted advertising, sale, sensitive data, certain profiling	Required for targeted advertising, sale, sensitive data, certain profiling	Annual cybersecurity audit and risk assessment requirements to be determined through regulations	N/A