MAYER | BROWN

March 25, 2022

Legal Update

Utah Passes Comprehensive Privacy Law: How the UCPA Compares to Other State Privacy Laws

Following in the footsteps of California, Virginia and Colorado, Utah has become the fourth state to pass comprehensive consumer data privacy legislation. The Utah Consumer Privacy Act ("UCPA") was introduced on February 17, 2022, passed through the Utah Senate unanimously in just one week (February 25, 2022) and passed out of the Utah House the next week (March 2, 2022), again unanimously. Utah Governor Spencer Cox signed the bill (SB 227) into law on March 24, 2022, and the UCPA will take effect on December 31, 2023. The swift and unanimous passage of a complex, comprehensive data privacy law would be remarkable under any circumstances, but the UCPA's rapid enactment is particularly noteworthy given the number of state law proposals that remain bogged down (e.g., Arizona, Georgia, Maine) or that died (e.g., Florida, Indiana, Mississippi) already this year. While bills are still alive in some other states (e.g., Alaska, Connecticut, Ohio, Pennsylvania), Utah is the first major state law domino to fall in 2022 and the first state to enact comprehensive data privacy legislation since Colorado in July 2021.

Companies that followed the passage of the California Consumer Privacy Act ("CCPA"), the California Privacy Rights Act ("CPRA"), Virginia's Consumer Data Protection Act ("VCDPA") and the Colorado Privacy Act ("CPA") likely will not struggle to meet the familiar requirements set out by the UCPA. Similar to the VCDPA and CPA, Utah's UCPA adopts the "controller" and "processor" nomenclature used in the EU General Data Protection Regulation ("GDPR") and does not include a private right of action for consumers to sue for potential violations. Also like the GDPR and the other state frameworks, the UCPA grants consumers certain rights over their personal data.

However, the UCPA has some key distinctions. For example, the UCPA does not grant consumers the right to correct inaccuracies in their personal data and does not require controllers to conduct data protection assessments of certain processing activities. And unlike the VCDPA and CPA, both of which require opt-in consent for the collection and processing of "sensitive data," the UCPA instead requires covered entities to provide notice and an opportunity to opt-out prior to processing a consumer's "sensitive data."[1] Further, instead of getting routed directly to the Utah Attorney General ("AG"), consumer complaints first go to the Utah Division of Consumer Protection within the Utah Department of Commerce, which may refer complaints to the AG. Neither the AG nor the Division of Consumer Protection have explicit rulemaking authority under the statute.

Scope

The UCPA covers for-profit entities that conduct business in Utah—or produce a product or service targeted to Utah residents—that (1) have annual gross revenues of at least $25 million and (2) either (i) control or process the personal data of at least 100,000 Utah residents or (ii) derive over 50 percent of gross revenue from the "sale" of personal data and control or process personal data of at least 25,000 residents.[2] Covered businesses are considered either a "controller" or a "processor" under the UCPA's statutory scheme.[3]

The UCPA defines "consumer" as an individual who is a resident of Utah acting in an individual or household context and only applies to the personal data of consumers—not personal data collected in an employment or commercial (business-to-business) context. The UCPA defines "personal data" as information linked or reasonably linkable to an identified or identifiable individual, with exceptions for de-identified data, aggregated data and publicly available information. Entities subject to the UCPA need not re-identify de-identified or pseudonymous data in order to comply with the statute's obligations.

Exemptions

Like the CCPA, CPRA, VCDPA and CPA, the UCPA exempts certain types of data and certain entities. Notably, the UCPA exempts information and entities regulated by both the Health Insurance Portability and Accountability Act ("HIPAA") and the Gramm-Leach-Bliley Act ("GLBA"), institutions of higher education, non-profits, tribes and consumer reporting agencies subject to the Fair Credit Reporting Act ("FCRA").

COMPARING EXEMPTIONS IN STATE PRIVACY LAWS

Exemption	UCPA	CPA	VCDPA	CPRA	CCPA
Financial institutions and data subject to GLBA	Both exempt	Both exempt	Both exempt	Institutions not exempt, Data exempt*	Institutions not exempt, Data exempt*
Covered entities/business associates and protected health data under HIPAA and HITECH	Both exempt	Data exempt	Both exempt	Limited entities exemption, Data exempt*	Limited entities exemption, Data exempt*
Personal information subject to FCRA	Exempt	Exempt	Exempt	Exempt	Exempt
Employee/applicant personal data within employment context	Exempt	Exempt	Exempt	Exempt from most obligations until 1/1/2023*	Exempt from most obligations until 1/1/2023*
Personal data within business (B2B) context	Exempt	Exempt	Exempt	Exempt until 1/1/2023*	Exempt until 1/1/2023*
Non-profits	Exempt	Not exempt	Exempt	Exempt	Exempt
Institutions of higher education	Exempt	Exempt if non-profit	Exempt	Exempt if non-profit	Exempt if non-profit

* Subject to private right of action in the context of a data breach.

Data Subject Rights

The UCPA, like its counterparts, provides consumers with rights relating to personal data processed by controllers and processors, rights which consumers may request to exercise using methods specified by the controller in the required privacy notice. These consumer rights include:

- Confirmation that a controller is processing the consumer's personal data
- Access to the consumer's personal data
- Deletion of the personal data that the consumer provided to the controller
- Data portability: the right to obtain a copy of the personal data, in a "portable" format, that the consumer provided to the controller
- Opt-out of the "sale" of personal data or the processing of personal data for targeted advertising

Notably, like the CCPA and CPRA, the UCPA limits the consumer deletion right to personal data that the consumer provided to the controller. And disclosure of personal data to third parties is not considered a sale if the purpose is consistent with a consumer's reasonable expectations.

COMPARING CONSUMER RIGHTS UNDER STATE PRIVACY LAWS

Exemption	UCPA	CPA	VCDPA	CPRA	CCPA
Access	Yes	Yes	Yes	Yes	Yes
Correct	Yes	Yes	Yes	Yes	No
Delete	Yes (limited to data that consumer provided to controller)	Yes (personal data concerning consumer)	Yes (data provided by or obtained about consumer)*	Yes (data collected from consumer)	Yes (data collected from consumer)
Portability	Yes	Yes	Yes	Yes	Yes
Opt-out of sale	Yes	Yes	Yes	Yes	Yes
Non-discrimination	Yes	Yes	Yes	Yes	Yes
Appeals process	No	Yes	Yes	No	No

* Recognizing the operational difficulties that indirect data collectors face in processing deletion requests, Virginia has passed a bill (HB 381) permitting businesses that collect data indirectly about (rather than directly from) a consumer to opt the consumer out of processing as an alternative to deletion or to retain the minimal data necessary to ensure effective deletion. The Virginia Governor has until April 11, 2022 to act on the bill.

Data Controller and Processor Obligations

Like the VCDPA and CPA, the UCPA adopts the "controller" and "processor" structure set forth in the GDPR. Before a processor performs any processing on behalf of a controller, the UCPA requires the parties to enter into a contract establishing the details of the processing, along with the parties' rights and obligations. The agreement must set forth:

- Instructions for the processing

- The nature and purpose of the processing
- The type of data subject to processing
- The duration of the processing

Processors must adhere to the instructions of the controller and take appropriate technical and organizational measures to assist the controller in meeting its obligations, including as related to security of personal data and breach notification. The data processing contract also must set forth the following processor obligations:

- Follow the controller's instructions when processing data
- Ensure that all persons handling personal data are subject to a duty of confidentiality with respect to the personal data
- Engage any subcontractors via a written agreement that requires the subcontractor to meet the same obligations as the processor with respect to the personal data

In addition, the UCPA requires controllers to provide consumers with a reasonably accessible and clear privacy notice. But, unlike the CPA, VCDPA and CPRA, the UCPA does not require controllers to conduct data protection assessments of certain processing activities. The privacy notice must disclose:

- Categories of personal data processed by the controller
- Purposes for such processing
- How consumers can exercise their rights under the law
- Categories of personal data that the controller shares with third parties
- Categories of third parties with whom the controller shares personal data

DATA CONTROLLER OBLIGATIONS UNDER STATE PRIVACY LAWS

Exemption	UCPA	CPA	VCDPA	CPRA	CCPA
Data minimization	Yes	Yes	Yes	Yes	No
Purpose limitation	Yes	Yes	Yes	Yes	Yes
Security requirements	Yes	Yes	Yes	Yes	No, but the private right of action applies to security breaches
Consent for sensitive data	No, consumers can opt-out	Yes	Yes	No, consumers can limit use to what is reasonably necessary	No
Special requirements for children's data	Yes (personal data for a known child under 13 years)	Yes (personal data for a known child under 13 years)	Yes (sensitive data of children under 13 years)	Yes (sale of personal information of children under 16 years)	Yes (sale of personal information of children under 16 years)
Privacy notice	Yes	Yes	Yes	Yes	Yes
Disclose sale	Yes	Yes	Yes	Yes	Yes

Exemption	UCPA	CPA	VCDPA	CPRA	CCPA
Data protection assessment	No	Yes, available upon request by CO AG	Yes	Yes, risk assessments submitted to CA Privacy Protection Agency	No
Requirements for de-identified data	Yes	Yes	Yes	Yes	Yes

Effective Dates and Enforcement

The UCPA's enactment adds to an evolving timeline of data privacy laws and regulations. The CCPA and its implementing regulations, of course, are already in effect and enforceable. The CPRA becomes operative January 1, 2023, and enforceable on July 1, 2023, along with regulations to be adopted by the new California Privacy Protection Agency ("CPPA") on or before July 1, 2022 (however, the draft regulations are currently past due for public notice and comment, and the CPPA executive director has acknowledged that draft regulations may be delayed until fall 2022). Likewise, the Colorado AG has announced that his office will issue a notice of rulemaking and draft regulations by fall 2022, to be finalized and adopted by July 1, 2023, when the CPA takes effect. The VCDPA, meanwhile, takes effect January 1, 2023, without rulemaking or regulations. The UCPA is now the latest entry on the data privacy law calendar, taking effect on December 31, 2023, also without rulemaking or regulations.

The UCPA expressly does not create a private right of action. Rather, the AG is given the exclusive authority to enforce the statute, but only on referral from the Utah Division of Consumer Protection, which can receive and investigate complaints and provide consultation and assistance to the AG. The AG must give businesses 30 days to cure alleged violations, after which, if no cure, the AG can bring an action to recover actual damages (to the consumer) and statutory penalties of up to $7,500 per violation of the statute.[4] All recovered funds go to the newly created Consumer Privacy Account, which will be used to fund future enforcement efforts and offset enforcement fees and costs. The AG and the Division of Consumer Protection must compile a report evaluating the UCPA's liability and enforcement provisions and summarizing the data protected and not protected by the statute and submit the report to Utah's Business and Labor Interim Committee by July 1, 2025. Given that only 18 months will pass between the effective date of the UCPA and the required issuance of the report summarizing its effectiveness, we may reasonably expect significant activity from the Division of Consumer Protection and the AG. These agencies may take relatively more concerted action to conduct investigations and bring enforcement actions in order to demonstrate their effectiveness in exercising the new authorities conveyed to them by the UCPA.

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

Vivek K. Mohan
+1 650 331 2054
vmohan@mayerbrown.com

Mark Bonham
+1 801 907 2702
mbonham@mayerbrown.com

Rajesh De
+1 202 263 3366
rde@mayerbrown.com

Samuel P. Gardiner
+1 801 907 2701
sgardiner@mayerbrown.com

Philip R. Recht
+1 213 229 9512
precht@mayerbrown.com

Scott F. Young
+1 801 907 2710
syoung@mayerbrown.com

Evan M. Wooten
+1 213 621 9450
ewooten@mayerbrown.com

Joshua M. Cohen
+1 312 701 8198
jmcohen@mayerbrown.com

Britteny L. Leyva
+1 213 229 5107
bleyva@mayerbrown.com

Endnotes

[1] "Sensitive data" is defined as (i) personal data that reveals an individual's racial or ethnic origin, religious beliefs, sexual orientation, citizenship or immigration status, or information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional; (ii) processing of genetic personal data or biometric data for the purpose of identifying a specific individual; or (iii) specific geolocation data.

[2] "Process" is defined as an operation or set of operations performed on personal data, including collection, use, storage, disclosure, analysis, deletion or modification.

[3] "Controller" is defined as a person doing business in the state who determines the purposes for which and the means by which personal data is processed, regardless of whether the person makes the determination alone or with others. "Processor" is defined as a person who processes personal data on behalf of a controller.

[4] The CPRA authorizes, but does not require, the CPPA to allow companies to cure violations. The cure periods for Virginia (30 days) and Colorado (60 days) are mandatory; although in Colorado, the cure provision expires on January 1, 2025.