MAYER | BROWN

May 11, 2022

Legal Update

Connecticut Passes Comprehensive Privacy Law: Comparing to Other State Privacy Laws

Following the lead of California, Virginia, Colorado and, most recently, Utah, Connecticut has become the fifth state to pass comprehensive consumer data privacy legislation. The Connecticut legislature passed "An Act Concerning Personal Data Privacy and Online Monitoring" (referred to in this Legal Update as the "Connecticut Data Privacy Act" or "CTDPA") on April 28, 2022. Connecticut Governor Ned Lamont signed the bill (SB 6) into law on May 10, 2022, and the CTDPA will take effect on July 1, 2023. Connecticut is the second state to enact such a law in in 2022, following in the footsteps of the Utah Consumer Privacy Act ("UCPA"), which was signed into law on March 24, 2022, and will take effect on December 31, 2023.

Companies that have followed the California Consumer Privacy Act ("CCPA"), the California Privacy Rights Act ("CPRA"), Virginia's Consumer Data Protection Act ("VCDPA"), the Colorado Privacy Act ("CPA") and the UCPA will find many similarities in the CTDPA. Similar to the other non-California laws, the CTDPA 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. Nor does the CTDPA extend consumer rights to the employee or business-to-business context. The CTDPA grants applicable consumers certain familiar rights, including to access, correct and delete their personal data.

The CTDPA is arguably less business-friendly and more consumer-oriented than the Virginia and Utah frameworks, aligning more closely with Colorado's law and in some ways with the California model. Similar to Colorado, the CTDPA requires controllers, starting January 1, 2025, to recognize consumers' opt-out preference signals for targeted advertising and sales, a mechanism often referred to as "global opt-out." (In California, once the CPRA takes effect, businesses will have the option, but not the obligation, to recognize opt-out preference signals while Utah and Virginia have no global opt-out provisions.) The CTDPA does not require controllers to authenticate consumer opt-out requests; rather, controllers may deny opt-out requests if it is unreasonably burdensome to associate the request with the personal data. Like California and Colorado, the CTDPA grants consumers the right to opt-out of personal data sales, targeted advertising, and profiling, and the CTDPA's definition of "sale" is similarly broad.[1] Also, like California and Colorado, the CTDPA's right for controllers to cure violations has an expiration date (December 31, 2024).

Notably, the CTDPA does not authorize the Connecticut Attorney General ("CT AG") to engage in rulemaking, although future rulemaking from Colorado and California on similar provisions may

influence the interpretation of such provisions in the CTDPA. Similar to Colorado and Virginia, the CTDPA requires opt-in consent for the collection and processing of "sensitive data";[2] however, the CTDPA also requires controllers to provide a mechanism for consumers to revoke this consent. Also, the CTDPA takes a hard line on children's data, requiring controllers to obtain consent to sell the personal data of a consumer between the ages of 13 and 16 or to process that data for targeted advertising.

Scope

The CTDPA applies to for-profit entities that conduct business in Connecticut—or produce products or services targeted to Connecticut residents—and that in the preceding year controlled or processed[3] the personal data of:

i. At least 100,000 Connecticut residents or

ii. At least 25,000 Connecticut residents and derived over 25 percent of gross revenue from selling personal data

The CTDPA protects "consumers," and covered businesses are referred to as "controllers" or "processors."[4]

The CTDPA does not apply to personal data collected in an employment or business-to-business context. "Personal data" is defined as information "linked or reasonably linkable to an identified or identifiable individual" and does not include de-identified data or publicly available information. Covered entities are not required to re-identify de-identified or pseudonymous data in order to comply with the statute.

Exemptions

Like the other comprehensive state laws, the CTDPA contains exemptions. In addition to not applying to entities that do not meet the size threshold, the CTDPA's obligations do not apply to state government agencies, covered entities and business associates regulated by the Health Insurance Portability and Accountability Act ("HIPAA"), financial institutions regulated by the Gramm-Leach-Bliley Act ("GLBA"), non-profits and institutions of higher education.

COMPARING EXEMPTIONS IN STATE PRIVACY LAWS

Exemption	CTDPA	UCPA	CPA	VCDPA	CPRA	CCPA
Financial institutions and data subject to GLBA	Both exempt	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	Both exempt	Data exempt	Both exempt	Limited entities exemption, Data exempt*	Limited entities exemption, Data exempt*
Personal information subject to FCRA	Data Exempt	Exempt	Exempt	Exempt	Exempt	Exempt
Employee/applicant personal data within employment context	Exempt	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	Exempt until 1/1/2023*	Exempt until 1/1/2023*
Non-profits	Exempt	Exempt	Not exempt	Exempt	Exempt	Exempt
Institutions of higher education	Exempt	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 CTDPA provides consumers with rights relating to their personal data that consumers may request to exercise using methods established by the controller and described in the controller's privacy notice. These rights include:

- Confirmation that a controller is processing the consumer's personal data and access to the consumer's personal data unless such confirmation or access "would require the controller to reveal a trade secret"
- Correction of inaccuracies in the consumer's personal data
- Deletion of the personal data provided by, or obtained about, the consumer
- Data portability: the right to obtain a copy of the consumer's personal data in a "portable" and "readily usable" format
- Opt-out of the processing of the consumer's personal data for purposes of (i) targeted advertising, (ii) sale or (iii) profiling in furtherance of automated decision-making

COMPARING CONSUMER RIGHTS UNDER STATE PRIVACY LAWS

Right	CTDPA	UCPA	CPA	VCDPA	CPRA	CCPA
Access	Yes	Yes	Yes	Yes	Yes	Yes
Correct	Yes	No	Yes	Yes	Yes	No
Delete	Yes (data provided by or obtained about consumer*)	Yes (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	Yes
Opt-out of sale	Yes	Yes	Yes	Yes	Yes	Yes
Non-discrimination	Yes	Yes	Yes	Yes	Yes	Yes
Appeals process	Yes	No	Yes	Yes	No	No

* The CTDPA authorizes businesses that collect data indirectly (about, rather than from, a consumer) to opt the consumer out of processing as an alternative or to retain (suppress) minimal data to ensure continued deletion. The VCDPA was amended on April 11, 2022, in like fashion.

Data Controller and Processor Obligations

Like the other non-California frameworks, the CTDPA adopts the "controller" and "processor" structure set forth in the GDPR. The CTDPA requires a processor to adhere to the controller's instructions and assist the controller in meeting its obligations under the statute. The parties must enter into a binding contract that governs the processor's data processing procedures on behalf of the controller. The contract must include:

- Instructions for the processing
- Nature and purpose of the processing
- Type of data subject to processing

- Duration of the processing
- Rights and obligations of both parties
- Requirement that each person processing personal data is subject to a duty of confidentiality
- Requirement for the processor to delete or return the personal data at the controller's direction at the end of the provision of services
- Commitment to engage any subcontractors, after providing the controller an opportunity to object, via a written contract that requires the subcontractor to meet the obligations of the processor
- Commitment to cooperate with reasonable data security assessments by the controller or a designated third party

In addition, the CTDPA requires controllers to conduct and document a data protection assessment for each processing activity "that presents a heightened risk of harm to a consumer." Such processing activities include (i) processing for purposes of targeted advertising, (ii) sale of personal data, (iii) processing for purposes of profiling and (iv) processing of sensitive data. The CT AG may require that a controller disclose any data protection assessment relevant to a CT AG investigation.

DATA CONTROLLER OBLIGATIONS UNDER STATE PRIVACY LAWS

Obligation	CTDPA	UCPA	CPA	VCDPA	CPRA	CCPA
Data minimization	Yes	Yes	Yes	Yes	Yes	No
Purpose limitation	Yes	Yes	Yes	Yes	Yes	Yes
Security requirements	Yes	Yes	Yes	Yes	Yes	No, but the private right of action applies to security breaches
Consent for sensitive data	Yes	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 (sale of personal information of children under 16 years)	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	Yes
Disclose sale	Yes	Yes	Yes	Yes	Yes	Yes
Data protection assessment	Yes	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	Yes

Effective Dates and Enforcement

The CTDPA adds to a growing timeline of comprehensive consumer privacy laws and regulations. The CCPA and its implementing regulations are already in effect. 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"). Draft CPRA regulations have been delayed until fall 2022. The Colorado AG also plans to issue draft regulations by fall 2022, to be finalized and adopted by July 1, 2023, when the CPA takes effect. The VCDPA (effective January 1, 2023) and UCPA (effective December 31, 2023) do not feature rulemaking or regulations. The CTDPA will slot in between the VCDPA and UCPA, taking effect on July 1, 2023, albeit without interpretive rulemaking or regulations.

Effective Date	CTDPA	UCPA	CPA	VCDPA	CPRA	CCPA
January 1, 2020						✓
January 1, 2023				✓	✓	
July 1, 2023	✓		✓			
December 31, 2023		✓				

The CTDPA explicitly does not create a private right of action for statutory violations. The CT AG has "exclusive authority" to enforce the law. For the first 18 months (from July 1, 2023 to December 31, 2024), the CT AG must issue a notice of violation to the controller and provide an opportunity to cure the alleged violation within 60 days of receipt of the notice. Beginning January 1, 2025, the CT AG has discretion to grant such an opportunity to cure an alleged violation. Statutory violations of the CTDPA constitute an unfair trade practice under the Connecticut Unfair Trade Practices Act ("CUTPA"), which authorizes injunctive relief and civil penalties of up to $5,000 per violation for willful misconduct (i.e., the business knew or should have known the activities violated the law). Only the CT AG may bring suit under the CUTPA.

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

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

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

Arsen Kourinian
+1 213 229 5141
akourinian@mayerbrown.com

Dominique Shelton Leipzig
+1 213 229 5152
dsheltonleipzig@mayerbrown.com

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

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

Endnotes

[1] "Sale of personal data" is defined as the exchange of personal data for monetary or other valuable consideration by the controller to a third party.

[2] "Sensitive data" is defined as personal data that includes (A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, or citizenship or immigration status, (B) the processing of genetic or biometric data for the purpose of uniquely identifying an individual, (C) personal data collected from a known child, or (D) precise geolocation data.

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

[4] "Consumer" is defined as an individual who is a resident of Connecticut. "Controller" is defined as an individual or legal entity that alone or jointly with others determines the purpose and means of processing personal data. "Processor" is defined as an individual or legal entity that processes personal data on behalf of a controller.