DAVIS GILBERT

Connecticut Becomes Fifth State To Pass Comprehensive State Privacy Law

The Bottom Line

- Connecticut is the fifth state to enact a comprehensive consumer privacy law, but it certainly will not be the last.
- This new law adopts many themes from previous state laws, but as we are seeing, these laws all have unique aspects and are not identical to one another. As a result, privacy compliance in the United States continues to get more complex.

The seemingly relentless passage of state privacy legislation continues as Connecticut enacts its own comprehensive consumer privacy regulation. On May 10, 2022, Governor Ned Lamont signed into law An Act Concerning Personal Data Privacy and Online Monitoring (CTDPA). The new law will go into effect on July 1, 2023, the same date as the effective date of the new Colorado privacy law.

Threshold Requirements

The CTDPA applies to persons that conduct business in the state or produce products or services targeted to state residents and, during the prior calendar year, controlled or processed the personal data of:

- 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
- 25,000 consumers and derived over 25% of gross revenue from the "sale" (defined as "the exchange of personal data for monetary or other valuable consideration") of personal data.

The exclusion of payment transactions is unique to the CTDPA, and should be helpful to retailers and other small businesses that only use credit and debit card information to facilitate sales. Moreover, the 25% revenue threshold for personal data sales is significantly lower than the 50% required by the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), the Virginia Consumer Data Protection Act (VDCPA), and the Utah Consumer Privacy Act (but not the Colorado Privacy Act (CPA), which is triggered if the controller derives any revenue at all).

Consumer Rights

As with the other new state privacy regimes, the CTDPA provides consumers with a series of rights regarding their personal data: rights of access, correction, deletion, and data portability; and the right to opt out of targeted advertising, sales of personal data, and profiling for "solely automated decisions that produce legal or similarly significant effects concerning the consumer." Similar to the CPRA and CPA, the CTDPA recognizes global device settings as a method for consumers to exercise their opt-out rights. By January 1, 2025, controllers are required to allow consumers to use opt-out preference signals to opt out of the sale of

their personal data or any processing used for targeted advertising. The CPRA is the only other state law to expressly recognize opt-out preference signals.

Additionally, the CTDPA is unique in not requiring controllers to authenticate opt-out requests (although controllers may deny such requests if reasonably suspected to be fraudulent). The intent behind this provision may be to reduce the ability of businesses to thwart the exercise of consumer rights by imposing burdensome authentication requirements. The waiver of authentication does not extend to other consumer rights, such as access, correction, deletion, and data portability.

Children and Teenagers

While controllers are already required to process the data of children younger than 13 in accordance with the Children's Online Privacy Protection Act (COPPA), the CTDPA further prohibits sales of personal data or processing for targeted advertising without consent if the consumer is at least 13 years old but younger than 16, and the controller has actual knowledge of or willfully disregards the consumer's age. The CCPA, with its "right to opt-in," is currently the only other state privacy law that has a similar requirement.

Additionally, the Connecticut law treats "personal data collected from a known child" as sensitive data, analogous to Virginia and Colorado, and the processing of such data triggers the requirement to conduct a data protection assessment (see below). Finally, the law requires the Connecticut General Assembly, by September 1, 2022, to convene a task force to study "[a]ny means available to verify the age of a child who creates a social media account," suggesting a potential focal point of Connecticut's enforcement priorities.

Data Protection Assessments; Data Protection Agreements

Similar to the new laws in California, Virginia and Colorado (but notably not Utah), the Connecticut law requires companies to conduct and document a "data protection assessment" of activities that present "a heightened risk of harm to a consumer" by identifying and weighing the benefits of the processing to the potential risks that it poses to consumer rights. Activities requiring a data protection assessment include:

- Sales of personal data;
- Processing personal data for targeted advertising;
- Profiling that presents certain risks to the consumer; and
- Processing sensitive data.

Unlike the CPRA's rule requiring businesses to submit mandatory "risk assessments" to California regulators on a "regular basis," the CTDPA requires that companies make data protection assessments available to the Connecticut Attorney General only upon request.

The CTDPA also follows the lead of some prior state privacy laws by requiring that data controllers and data processors enter into a contract regarding the processing of the personal data. This trend of statutorily-required contracts will likely lead companies to revisit their agreements with various service providers.

Sensitive Data

Like the comprehensive state privacy laws in Virginia and Colorado, the CTDPA requires that, if a business is processing "sensitive data" from a consumer, the business must obtain opt-in consent. Under the CTDPA, "sensitive data" includes:

- Data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status;
- Genetic or biometric data (if used for the purpose of uniquely identifying an individual);
- Personal data collected from a known child; or
- Precise geolocation data (within a radius of 1,750 feet or less).

Enforcement

The CTDPA is enforceable solely by the Connecticut Attorney General. The law expressly states that it does not create a private right of action. Echoing Colorado's enforcement framework, violations of the CTDPA constitute a per se "unfair trade practice" under the existing Connecticut Unfair Trade Practices Act.

For the first 18 months from the law's effective date, the Attorney General must issue companies a notice of violation and grant them 60 days to cure such violation before bringing an enforcement action. However, beginning Jan. 1, 2025, the Attorney General will have discretion over whether to grant such opportunity to cure by considering:

- The number of violations;
- The size and complexity of the controller or processor;
- The nature and extent of the controller's or processor's processing activities;
- The substantial likelihood of injury to the public;
- The safety of persons or property; and
- Whether such alleged violation was likely caused by human or technical error.

The sunsetting of the CTDPA's notice-and-cure provision, combined with similar provisions under the CPRA and CPA, will allow Connecticut to join multistate investigations and enforcement actions with California and Colorado for privacy violations under their new privacy frameworks. However, the laws in Virginia and Utah, which do not have an expiration date for their notice-and-cure periods, will make it difficult to engage in joint activity with those states.

Related People

Gary Kibel
Partner
212 468 4918
gkibel@dglaw.com

Zachary N. Klein
Associate
212 237 1495
zklein@dglaw.com