

TYPES NOT MAPPED YET May 27, 2022 | TTR not mapped yet | Elizabeth (Libby) A. James, Luke Sosnicki

# Utah and Connecticut enact comprehensive data privacy laws

Connecticut and Utah both enacted comprehensive privacy laws this spring. On March 24, 2022, Utah became the fourth state to enact a comprehensive data privacy law when Governor Spencer Cox signed [Senate Bill 227](#), known as the Utah Consumer Privacy Act ("UCPA"). Connecticut Governor Ned Lamont signed Public Act No. 22-15, ["An Act Concerning Personal Data Privacy and Online Privacy"](#) on May 10.

## Utah

Many of the rights created for Utah consumers by the UCPA are similar to rights seen in other states' data privacy laws. The definitions included with the law are similar to ones seen in previous state privacy laws in Colorado and Virginia. The law applies to businesses that are either a "processor" or a "controller" of personal data—borrowing terminology from the European Union's General Data Protection Regulation ("GDPR") much as laws in Virginia and Colorado have done. Unlike either the GDPR or the Colorado and Virginia laws, however, fewer businesses are covered by the UCPA even if they otherwise would qualify as a "controller" and/or "processor." This is because only businesses that have an annual revenue of \$25 million or more and reach certain data-level thresholds are covered by the UCPA. A business can reach these thresholds either by controlling/processing the personal data of 100,000 or more consumers per year, or by both deriving over 50% of its gross revenue from the sale of personal data *and* controlling/processing the data of 25,000 or more customers. So a business that processes/controls the personal data of between 25,000 and 99,999 consumers per year—automatically covered under the Colorado data privacy law, for example—would be exempt from the UCPA unless it also has revenue of \$25 million or more per year, over 50% of which is derived from controlling/processing personal data.

The enforcement mechanism of the UCPA is different than ones employed by other state privacy statutes. The law first gives the Division of Consumer Protection ("DCP") (contained within the Utah Department of Commerce) the power to investigate any consumer complaints about potential violations of the law. After investigation, if the Division of Consumer Protection deems the claim legitimate then it must refer the matter to the Utah Attorney General. The Attorney General's office then conducts a second review, and may either concur with the findings of the DCP or dismiss the consumer's complaint as lacking merit. Although this might lead to a protracted review process, the existence of two levels within the UCPA's enforcement mechanism might also lead to fewer complaints in which a violation is determined to have occurred. The UCPA does not create a private cause of action, meaning that consumers who allege that a business has violated the statute do not have an independent right to sue under the UCPA alone.

The UCPA will go into effect on December 31, 2023.

## Connecticut

Connecticut's law closely mirror the other states' data privacy laws as well in terms of its substance and what types of businesses and transactions it covers. The law applies to entities that either control and/or process personal data of 100,000 consumers or more per year, or control and/or process personal data of 25,000 consumers or more per year if that entity derives more than 25% of its gross revenue from selling personal data.

The Connecticut law gives consumers the right to know whether a business collects data about them, as well as to request corrections to or deletion of their personal data controlled by the business. The law also gives consumers the right to opt out of data collection and processing for the purposes of targeted advertising, sale, or automated decision-making based on data profiling—all opt-outs that are similar to provisions in other states' comprehensive data privacy laws. The law creates affirmative obligations for covered businesses to limit data processing to what is "reasonably necessary" for their purposes, provide a way for consumers to revoke their consent to data processing, and protect consumers' data with adequate cybersecurity practices. Similar to the Utah law, there is no private right



of action, but unlike Utah's multi-layered enforcement scheme, the law is enforced by the Connecticut Attorney General. One item worth noting is that the Connecticut Attorney General's Office has been among the nation's most active on privacy and cybersecurity matters over the last several years.

The Connecticut statute becomes effective July 1, 2023.

Thompson Coburn's attorneys are closely monitoring the developments in Utah and Connecticut and in the privacy landscape generally. For questions, please contact the Thompson Coburn lawyer with whom you usually work, the authors, or any member of the firm's [Cybersecurity, Privacy, and Data Governance](#) practice group.

#### authorsTest

**elizabeth**

Elizabeth (Libby) A. James

**luke**

Luke Sosnicki