DAVIS GILBERT

Privacy + Data Security

An (Im)Perfect 10: Indiana, Tennessee, Montana & Texas Pass Consumer Privacy Laws

The Bottom Line

- There are now 10 states with comprehensive privacy laws, with more on the way.
- Without federal legislation, a patchwork of state laws may be the standard going forward, much in the same way that data breach notification laws eventually became ubiquitous at the state level.

In the absence of federal comprehensive privacy legislation, state lawmakers are enacting privacy laws at a breakneck pace. Following California, Virginia, Colorado, Utah, Connecticut and Iowa, four more U.S. states — Indiana, Tennessee, Montana and Texas — have put comprehensive privacy legislation on the books. While these laws are more similar than not, there are still inconsistencies and unique aspects of each that need to be considered. Perhaps most importantly, this trend brings more regulators to the table seeking to enforce their new laws against businesses.

Indiana

Gov. Eric Holcomb signed the Indiana Consumer Data Protection Act (ICDPA) into law on May 1, 2023. The ICDPA, which takes effect on January 1, 2026, will apply to businesses that control or process the personal data of at least: 100,000 consumers; or 25,000 consumers, and derive more than 50% of their gross revenue from personal data sales. With 2.5 years separating the law's passage and its effective date, the ICDPA gives businesses the longest period of time to prepare for compliance. While the ICDPA provides similar rights of access, deletion and correction as many of the other state laws, it uniquely allows data controllers to respond to a data portability request by providing either: (1) a copy of the personal data provided by the consumer; or (2) a "representative summary" of such data. The law's 30-day notice-and-cure period, similar to the laws in Virginia, Utah and Iowa, does not have a sunset date.

Tennessee

The Tennessee Information Protection Act (TIPA) was signed into law by Gov. Bill Lee on May 11, 2023, and will take effect on July 1, 2025. The threshold for coverage by the TIPA is narrower than any of the other state laws, applying to companies that make more than $25 million in revenue *and* control or process the personal information of at least: (1) 175,000 consumers; or 25,000 consumers, and derive more than 50% of their gross revenue from personal information sales. Additionally, the law's 60-day notice-and-cure period does not expire.

The most unique feature of the TIPA is the introduction of an affirmative defense against enforcement for organizations that implement and adhere to written privacy programs that comply with the National Institute of Standards and Technology (NIST) privacy framework or comparable privacy standards, and any future revisions to such frameworks. In determining the appropriateness of an organization's privacy program for the purposes of the affirmative defense, the TIPA considers the program's size and complexity, the nature and scope of its activities, the sensitivity of the information processed, the cost and availability of tools to improve privacy protections and data governance and compliance with comparable state or federal laws. The law also considers whether the organization certifies to the Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules or Privacy Recognition for Processors systems.

Montana

Gov. Greg Gianforte signed the Montana Consumer Data Privacy Act (MCDPA) into law on May 19, 2023. It will take effect on October 1, 2024. Given Montana's smaller population, the threshold for coverage under the MCDPA is lower than typical, applying to entities that control or process the personal data of at least: 50,000 consumers (approximately 4.5% of the state's population); or 25,000 consumers, and derive more than 25% of their gross revenue from personal data sales. The MCDPA most resembles Connecticut's law, which trends on the more consumer-friendly side of the spectrum, and has few distinguishing features that set it apart from the constellation of other state privacy laws. Controllers must recognize opt-out preference signals and conduct data protection assessments starting January 1, 2025, and the law's 60-day notice-and-cure period sunsets on April 1, 2026.

Texas

On May 28, 2023, the Texas Legislature passed the Texas Data Privacy and Security Act (TDPSA), which was ratified as of June 9, 2023, and will become effective on July 1, 2024.

The TDPSA has the broadest scope of coverage compared to any of the state laws enacted thus far. Instead of the typical monetary or numeric thresholds, the TDPSA applies to organizations that meet the following criteria:

- Conducts business in Texas or generates products or services *consumed* by (as opposed to targeted to) Texas residents;
- Processes or engages in the sale of personal data; and
- Does not qualify as a "small business," defined by the U.S. Small Business Administration as "an independent business having fewer than 500 employees" (however, small businesses must still obtain opt-in consent to sell consumers' sensitive personal data, even if exempt from the rest of the law).

The combination of these three criteria, which are completely new and unique to the state privacy landscape, will likely extend the law's purview to companies that would otherwise fall outside the scope of the California Consumer Privacy Act or other state laws.

Additionally, the TDPSA requires that companies expressly disclose that they "may sell" consumers' sensitive and/or biometric personal data, respectively. The TDPSA specifies that such disclosures "must be posted in the same location and in the same manner as the privacy notice, although it is unclear whether "in the same location and in the same manner" means that the disclosures must be located within the privacy notice itself or shown independently.

Finally, in comparison to other states' notice-and-cure periods, which typically require a written statement that the alleged violation was cured and actions were taken to ensure no further violations, the TDPSA's 30-day period sets a more stringent standard, obligating businesses to certify that they have:

- cured the alleged violation;
- notified consumers that the privacy violation was addressed, if consumer contact information is available;
- provided supportive documentation to show how the privacy violation was cured; and
- made changes to internal policies, if necessary, to ensure that no such further violations will occur.

The TDPSA does not have an expiration date for its notice-and-cure period.

For More Information

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

Gary Kibel

Partner
212 468 4918
gkibel@dglaw.com

Zachary Klein

Associate
212 237 1495
zklein@dglaw.com