Montana and Tennessee Join National Trend to Pass Broad Consumer Privacy Legislation: Top 8 Questions for Businesses

Insights
4.26.23

Last week, Montana and Tennessee became the eighth and ninth states to pass comprehensive consumer privacy legislation. The bills were approved by the respective legislatures and are expected to soon be signed by governors of both states. If signed into law, they will require you to take a number of compliance steps, including updating your website privacy policy, reviewing how data is collected and shared through cookies and pixels on your website, implementing a process for consumers in these states to exercise their new rights, updating your contracts with vendors, and conducting a data protection assessment. While the Montana and Tennessee bills are similar in substance, there are some key ways they differ. But one thing is certain: Businesses must adapt to new consumer privacy rights and keep up with this trend that is sweeping the nation. California, Connecticut, Colorado, Indiana, Iowa, Utah, and Virginia have already enacted similar laws — and over a dozen other states are currently considering similar bills. Up next may be Hawaii, Oklahoma, and yes, even Texas! For now, here are the answers to your top eight questions about the latest bills in Montana and Tennessee.

1. When Will These Laws Take Effect?

Once signed by the respective governor, the Montana Consumer Data Privacy Act (MCDPA) will take effect on October 1, 2024, and the Tennessee Information Protection Act (TIPA) will take effect on July 1, 2025. By contrast, the Iowa law enacted last month takes effect on January 1, 2025, and the Indiana bill passed earlier this month would take effect on January 1, 2026.

2. Will the Montana and Tennessee Laws Apply to Your Business?

TIPA applies to any for-profit business (subject to certain exemptions) that (a) conducts business in Tennessee or produces products or services that are targeted to Tennessee, (b) exceeds $25 million in annual revenue, and (c) meets either one of two criteria:

- During a calendar year, the business controls or processes personal information of at least 175,000 Tennessee residents; or
- Controls or processes personal information of at least 25,000 Tennessee residents and derive more than 50% of gross revenue from the sale of personal information.

Conversely, the MCDPA applies to any for-profit business (subject to certain exemptions) that conducts business in Montana or produces products or services that are targeted to Montana residents and meets any one of two criteria:

- During a calendar year, the business controls or processes personal data of at least 50,000 Montana residents; or
- Controls or processes personal data of at least 25,000 Montana residents and derives more than 50% of gross revenue from the sale of personal data.

Personal information (which is the same as "personal data" in Montana) is defined broadly and includes data that you may not think of. This includes data that can directly or indirectly identify a consumer.

Data can indirectly identify an individual if it can reasonably be associated with other data to identify them. For example, an IP address collected by your website about its visitors may itself qualify as personal information, even though you are not actually collecting names or other direct identifiers that are traditionally referred to under other laws as personally identifiable information.

As a result, if you do business in Tennessee, make over $25 million in annual gross revenue, and your website receives an average of 480 unique visitors from Tennessee per day, in 365 days you would surpass the 175,000 threshold if the website is collecting data about those visitors that meets the definition. That same threshold would be surpassed in Montana with an average of 137 unique visitors to your website from Montana per day, without having to meet a minimum revenue threshold.

3. Are Employees Treated as Consumers Under These Laws?

No. Unlike in California, where the California Consumer Privacy Act treats all employees and job applicants as consumers, Montana and Tennessee lawmakers decided to follow the rest of the states that recently passed consumer privacy laws and fully exempt data collected in the employment context, whether from employees, job applicants, or independent contractors. This exemption for employee data subjects does not have a sunset. It is a permanent exemption.

4. Can Individuals Sue for Violations of MCDPA and TIPA?

No. There is no private right of action under either law that would allow individuals to sue for any violation. Both laws go a step further and state that a violation of the law cannot serve as the basis for any lawsuit under any other law – this may eliminate risk of an unfair business practice claim based on violation of this law. The state attorney general has exclusive authority to enforce the law. However, individuals can submit complaints and report violations to the state attorney general, and consumer complaints may trigger an investigation.

5. What Do These Laws Require?

Montana

Other notable provisions of the MCDPA include:

- Exclusions: The statute exempts, among other things, non-profits, government entities, institutions of higher education, financial institutions, and personal data governed by the GLBA, covered entities or business associates and information and data subject to HIPAA, information governed by FERPA, and certain information that is regulated by FCRA.
- B2B data: As with the other state laws, aside from the CCPA, the MCDPA excludes from its definition of "consumer" the data of individuals acting in a commercial context.
- Consumer rights: Consumer rights include: (1) the right to demand deletion of data; (2) the right to access data; (3) the right to correct data; (4) the right to data portability for data previously provided by the consumer; (5) opt-out rights for the purpose of targeted marketing, the sale of personal data, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer; and (6) the right to revoke consent.
- Authentication of requests: Controllers are not required to authenticate opt-out requests but may deny the request if the controller has a good faith, reasonable, and documented belief that the request is fraudulent.
- Right to appeal: If a consumer's request is denied, the controller must provide instructions for how to appeal the decision. Controllers must establish a process for consumers to appeal that must be conspicuously available and like the process for submitting requests to initiate action pursuant to the statute.
- Additional rights for children: Controllers may not, among other things, process the personal data of a consumer for the purpose of targeted marketing or sale of the data without consent if the controller has actual knowledge that the consumer is between 13-16 years old.
- Opt-out preference signals: The MCDPA will require businesses to recognize browser privacy signals. The deadline for doing so is January 2025.
- Data protection assessments: The MCDPA requires data protection assessments for each processing activity that presents a heightened risk of harm to a consumer, including for purposes of: (1) targeted advertising; (2) the sale of personal data; (3) the processing of personal data for the purposes of profiling in which the profiling presents certain reasonably foreseeable risks; (4) the processing of sensitive data. Controllers may use data protection assessments performed to comply with other state laws, as long as the assessment is reasonably similar in scope and effect to that required by the Montana law. Data protection assessment requirements must apply to processing activities created or generated after January 1, 2025.
- Penalties: The statute does not specify any specific penalties or capped damage amounts.
- Right to cure: The statute contains a 60-day cure period for violations that sunsets after April 1, 2026.
- Rulemaking: The statute does not contain any provision for rulemaking by the attorney general

- Rulemaking: The statute does not contain any provision for rulemaking by the attorney general.

Tennessee

Other notable provisions of the TIPA include:

- Exclusions: The TIPA does not apply to, among other entities, financial institutions and data subject to GLBA, covered entities or business associates and information governed by HIPAA, institutions of higher education, information regulated by FERPA, or certain information subject to FCRA.
- B2B data: The statute defines "consumers" to include only a natural person who is a resident of Tennessee and who is acting only in a personal context.
- Consumer rights: Consumer rights include: (1) the right to demand deletion of data; (2) the right to access data; (3) the right to correct data; (4) the right to data portability for data previously provided by the consumer; (5) the right to disclosure of information relating to the sale of personal information or disclosure of such information for a business purpose; and (6) opt-out rights for the purpose of the sale of personal data, and targeted advertising.
- Authentication requests: Controllers may decline to comply with a request if they cannot authenticate the request using commercially reasonable efforts.
- Right to appeal: If a consumer's request is denied, the controller must provide instructions for how to appeal the decision. Controllers must establish a process for consumers to appeal that must be conspicuously available, at no cost, and like the process for submitting requests to initiate action pursuant to the statute.
- Data protection assessments: The TIPA requires data protection assessments for the following processing activities involving personal information: (1) targeted advertising; (2) the sale of personal data; (3) for the purposes of profiling in which the profiling presents certain reasonably foreseeable risks; (4) the processing of sensitive data; and (5) processing activities involving personal information that present a heightened risk of harm to consumers. Controllers may use data protection assessments performed to comply with other state laws, as long as they have reasonably comparable scope and effect. Data protection assessment requirements must apply to processing activities created or generated after July 1, 2024.
- Penalties: The statute permits civil penalties of up to $7,500 for each violation, in addition to reasonable attorneys' fees and investigative costs, and other relief the court deems to be appropriate, as well as injunctive relief and a declaratory judgment that an act or practice violates the TIPA.
- Right to cure: The statute contains a 60-day cure period for violations.
- Privacy program requirements: The TIPA requires controllers or processors to create, maintain, and comply with a written privacy program that reasonably conforms to the NIST privacy framework. If businesses comply with this requirement, they will be entitled to an affirmative defense for alleged violations of the act.

6. What Are the Key Differences Between Montana and Tennessee?

The key differences between the Montana and Tennessee laws, which are similar in many respects, include:

- The TIPA will only apply to businesses with over $25 million in revenue, whereas the MCDPA does not have a revenue threshold for the law to apply.
- The TIPA's written privacy program requirement mandating conformance with the NIST privacy framework and creating an affirmative defense for alleged violations of the TIPA.
- The MCDPA's requirement that businesses recognize opt-out preference signals, similar to requirements in California, Colorado, and Connecticut.
- The MCDPA's expansion of privacy rights for children between the ages of 13 and 16. This is also similar to the California and Connecticut statutes.
- The sunsetting of the right-to-cure period under the MCDPA. The TIPA's right to cure does not sunset.
- The lack of any verification requirement for opt-out requests under the MCDPA. The TIPA requires authentication of requests.

7. What Other State Consumer Privacy Laws Are on the Horizon?

So far, nine states have either enacted a comprehensive consumer privacy law or passed legislation expected to be signed by the respective state's governor. They are listed here in the order in which they either took or will take effect:

1. California: The California Consumer Privacy Act (CCPA) took effect January 1, 2020, with significant changes to the law taking effect January 1, 2023, and new regulations taking effect March 29, 2023.
2. Virginia: The Virginia Consumer Data Protection Act (VCDPA) took effect January 1, 2023.
3. Colorado: The Colorado Privacy Act (CPA) takes effect July 1, 2023.
4. Connecticut: Connecticut's Act Concerning Personal Data Privacy and Online Monitoring takes effect July 1, 2023.
5. Utah: The Utah Consumer Privacy Act (UCPA) takes effect December 31, 2023.
6. Montana: MCDPA will take effect October 1, 2024, pending the governor's signature.
7. Iowa: Iowa Senate File 262 was signed by the state governor on March 28, 2023 and takes effect on January 1, 2025.
8. Tennessee: TIPA will take effect July 1, 2025, pending the governor's signature.
9. Indiana: Indiana Senate Act No. 5 passed earlier this month and awaits the governor's signature. It is slated to take effect on January 1, 2026.

Fifteen states currently have active pending legislation similar in content to one or more of the above states. Of the fifteen states, the pending bills in Hawaii, New Hampshire, Oklahoma, and Texas appear to be advancing and might make it to the finish line in one form or another. The other states with pending legislation that appears to still be active this legislative session are Illinois, Louisiana, Massachusetts, Minnesota, New Jersey, New York, North Carolina, Oregon, Pennsylvania, Rhode Island, and Vermont.

8. What Should Businesses Do in the Meantime?

Businesses subject to the MCDPA or TIPA (or any of the other enacted laws outlined above) should take immediate action to develop a roadmap for compliance and begin executing on the plan. Compliance with these laws will take time and resources, so plan accordingly. The best place to start may be a gap assessment of your current data collection and privacy practices, as that would help identify immediate vs. long-term priorities. Completing your data inventory may be the next step, the results of which would feed into the drafting of compliant privacy notices and policies.

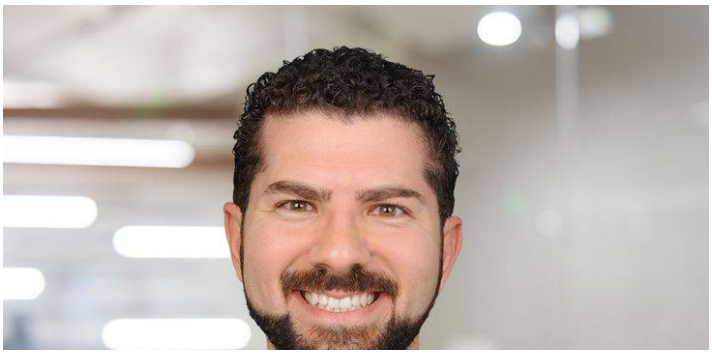
Need More Help?

With the help of Fisher Phillips' Consumer Privacy Team, your steps towards compliance can be fast-tracked. We are prepared to work with your team on a privacy gap assessment, data inventory, and drafting compliant privacy notices and policies for your business.

For further information, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on the firm's Consumer Privacy Team. Fisher Phillips will continue to monitor any obligations and enforcement efforts and provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox.

Want to learn more? Register for our upcoming webinar: The U.S. Data Privacy Landscape – Current State of Play. Join Risa Boerner (CIPP/US, CIPM), Usama Kahf (CIPP/US), and Anne Yarovoy Khan from the Fisher Phillips Consumer Privacy Team for a deep dive on data privacy regulations currently in effect and set to take effect across the US.

Related People



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email

Micah Dawson
Partner
303.218.3665
Email

Courtney Leyes
Partner
615.488.2902
Email

Service Focus

Consumer Privacy Team

Counseling and Advice

Privacy and Cyber

Related Offices

Nashville

Memphis