Baker McKenzie.

Client Alert

May 2023

State Consumer Privacy Laws Trending in 2023: Montana and Tennessee Join the Fold

After a slowdown in 2022--US states are back at the drawing board of consumer privacy laws with four passing in the last month alone. Here, we breakdown what you need to know about the Montana and Tennessee bills.

In brief

The early months of 2023 have brought a bumper crop of new state privacy legislation, with Tennessee and Montana legislatures poised to become the eighth and ninth states to enact comprehensive privacy laws. The Tennessee Information Protection Act and Montana Consumer Data Privacy Act, which both passed with unanimous votes out of their respective legislatures on April 21, 2023, follow the recent passage of privacy laws in Iowa and Indiana. The bills now land on their governors' desks for signature. While the bills hew to broad trends in state privacy laws, each contains novel provisions. Some of their key distinguishing features include:

- The new Montana law has lower than typical data-volume thresholds of applicability and will require businesses to acknowledge opt out preference signals after a sunrise period. Though the bill doesn't provide for private enforcement, it doesn't specify caps for monetary penalties.
- The Tennessee law will require in-scope businesses to implement a data security program that "reasonably conforms to" the NIST Privacy Framework, and adhering to this framework can also give a business an affirmative defense to protect against claims under the new law.

If enacted, the Montana and Tennessee bills will enter into force on October 1, 2024 and July 1, 2025, respectively.

Contents

Background
Montana Consumer Data Privacy Act
Tennessee Information Protection Act
Key takeaways
Contact Us

Background

The passage of the Tennessee and Montana bills on the same day consolidates the recent national trend of comprehensive state privacy legislation. While the whole of 2022 only saw the passage of two states' privacy laws (in Utah and Connecticut), in the past month alone four states have followed suit with new legislation. A beneficial similarity among all of the omnibus privacy statutes that have been enacted so far is that they distinguish between controllers (i.e., an entity that determines the means and purposes of processing personal data) and processors (i.e., an entity that processes personal data on behalf of a processor) and impose the bulk of their requirements on controllers.

A number of other states—including Oklahoma, Hawaii, and New Hampshire—are considering privacy bills that are in advanced stages of the legislative process. Additionally, Washington state recently passed the My Health, My Data Act, which will apply to personal information that is linked or reasonably linkable to a consumer and reasonably linkable to past, present, or future health status.

Montana Consumer Data Privacy Act

Scope: The Montana law will apply to businesses that produce products or services targeting Montana consumers and who either:

- control or process the personal data of at least 50,000 consumers (defined as Montana residents); or
- control or process the personal data of at least 25,000 consumers and who derive more than 25% of their gross revenue from the sale of personal data.

The law exempts state entities, nonprofit organizations, institutions of higher education, registered national securities associations, as well as entities governed by the privacy regulations of the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA). Businesses should take note of the lower than typical data-handling thresholds; by way of comparison, only businesses that process or control the data of at least in-state 100,000 consumers are subject to the Iowa and Virginia statutes. Both statutes also set the data-sale threshold at 50% of gross revenue, rather than the Montana law's 25%. This may have the effect of capturing some businesses that are out-of-scope of other state privacy laws and who will not have the advantage of relying on past compliance efforts. The Montana Consumer Data Privacy Act does not protect an individual acting in a commercial (i.e., B2B) or employment context.

Data subject rights: The Consumer Data Privacy Act establishes rights that will look familiar to anyone following recent state privacy legislation. Under the new act, consumers may confirm the processing of and access their personal data (subject to trade secret protection), correct inaccuracies in their personal data, request the deletion of personal data and obtain a copy of their data in readable format such that it may be ported to another controller. Controllers must respond to such requests without unreasonable delay and, in any case, within 45 days (the response period may be extended a further 45 days where necessary). Controllers must also not discriminate against consumers who exercise such rights, for example by charging different prices.

Consumers must also be given a means to opt out of certain types of processing: targeted advertising, the sale of their personal data (which is defined to include disclosures in exchange for money or other valuable consideration), and profiling based on automated decision-making that produces legally significant effects. By January 1, 2025, a controller must allow consumers to opt out of the sale of their personal information or targeted advertising through opt-out preference signals (i.e., universal opt out).

Processing: A controller may only process a consumer's personal data if it complies with certain conditions under the statute. Collection of personal data must be limited to that which is adequate, relevant and reasonably necessary for its stated purpose. In one of the more unique provisions of the new act (but not unique compared to California), controllers may only sell personal data of consumers between the ages of 13 and 15, or use their data for targeted advertising, if they have obtained their consent. Consent is also required for the processing of sensitive data—which includes data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, information about a person's sex life, sexual orientation, or citizenship or immigration status; genetic or biometric data; data collected from a known child; or precise geolocation data.

Privacy notice: Controllers must provide consumers with a clear and accessible privacy notice that includes the categories of data the controller processes, the purpose of the processing, the categories of data that is shared with third parties and the types of third parties with whom the data is shared, a contact email address, and instructions for exercising data subject rights. If personal data is sold to third parties or used for targeted advertising, the controller must clearly and conspicuously disclose the processing, along with a means for the consumer to opt out of such sale.

Controller-processor obligations: Contracts between controllers and processors must set out instructions for processing data, the nature and purpose of processing, the types of data being processed, the duration of processing, and the rights and obligations of the respective parties. The contract must also establish the processor's obligations to ensure that processing is conducted subject to a duty of confidentiality, to delete or return personal data at the end of the provision of services at the controller's direction, and to require subcontractors to meet all obligations of the processor with respect to the data.

Data security: Controllers must adopt administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. While the act doesn't prescribe specific measures, they should be appropriate considering the volume and nature of the data.

Data protection assessment: Controllers must conduct and submit a data assessment before engaging in certain activities deemed to present a heightened risk of harm to consumers. Such activities include targeted advertising, the sale of data, the processing of sensitive data, and processing that presents a reasonably foreseeable risk of unfair or deceptive treatment, financial, physical, or reputational injury, intrusion on private affairs, or other substantial injury. The controller may prepare a single data assessment for related processing activities or for complying with another law or regulation if it is similar in scope.

Enforcement: The Montana Consumer Data Privacy Act does not contain a private right of action and the attorney general has the exclusive enforcement authority. Until April 1, 2026, the attorney general will provide notice to a controller of any suspected violation of the act, giving the controller 60 days to correct the violation before commencing enforcement. After April 1, 2026, the attorney general can bring proceedings without notice. Unusually, the Montana Consumer Data Privacy Act does not specify the types of remedies available or provide limits on the monetary penalties that the attorney general may seek.

Tennessee Information Protection Act

Scope: The Tennessee act applies to businesses with revenue exceeding USD 25 million that offer products or services targeting Tennesseans and who control or process the personal information of at least 175,000 consumers (a notably higher threshold than the Montana act). The threshold for sellers of personal information is also slightly different than that in the Montana law;
Tennessee's Information Protection Act applies to businesses who control or process the personal information of at least 25,000 consumers and who derive more than 50% of their revenue from the sale of personal information (rather than Montana's, and most other states', 25% threshold). The proposed Tennessee law does feature familiar exemptions—such as state agencies, nonprofit organizations, institutions of higher education, registered national securities associations, and GLBA- and HIPAA-governed entities—but one of the more unique provisions is that licensed insurance companies are also exempt. The Information Protection Act also excludes persons acting in a commercial or employment context from the definition of "consumer".

Data subject rights: The Information Protection Act includes a similar litany of data subject rights. A consumer may confirm the processing of and access their personal information, correct inaccuracies, request the deletion of personal information and obtain a copy of their data. They may also request that a controller that has sold their personal information (defined to include disclosures in exchange for money or other valuable consideration) disclose (1) the categories of data sold, (2) the categories of third parties to which the data is sold, and (3) the categories of business information disclosed for a business purpose. Unlike the Montana law, such information is not required to be included in a controller's privacy notice (see below). Consumers must also be allowed to opt out of the sale of their data, targeted advertising and automated decision-making. Controller may also not discriminate against consumers who choose to exercise their data subject rights.

Processing: Like the Montana statute, the Information Protection Act embraces data minimization approaches to processing. Controllers should not collect or process personal information beyond what is adequate, relevant, and reasonably necessary for the purpose as stated to the consumer. As with the Montana Consumer Data Privacy Act, controllers may not process sensitive data, which is also defined similarly to the Montana law, without the consent of the consumer.

Privacy notice: The Information Protection Act privacy notice provisions are somewhat unusual in that they require that a controller provide a privacy notice on receipt of an authenticated consumer request. The notice should include the categories of personal information processed, the purpose of the processing, how consumers can exercise their rights, the categories of data that the controller sells to third parties, the categories of third parties to which the data is sold, and the right to opt out of the sale of information to third parties. A separate provision requires controllers to provide a privacy notice describing methods for consumers to submit a request to exercise their rights including either a toll-free number, email address, web form, or a link to a website that enables the submission of a data subject request.

Controller-processor obligations: The Tennessee act's rules on controller-processor contracts largely mirror those of Montana's and other existing state privacy laws. Controllers must ensure their contracts with processors outline instructions for processing data, the nature and purpose of processing, the types of data being processed, the duration of processing, and the rights and obligations of the respective parties. Likewise the processor should be required under the contract to ensure that processing is conducted subject to a duty of confidentiality, to delete or return personal information at tend of the provision of services at the controller's discretion, make available information to the controller to demonstrate the processor's compliance and to require subcontractors to meet all obligations of the processor with respect to the data.

Data protection assessment: The Information Protection Act's data protection assessment provisions largely mirror those of the Montana act and other existing state privacy laws. A controller must prepare an assessment before undertaking processing with a heightened risk of harm (the triggering activities are identical in substance to those in the Montana law, discussed above). The assessment should weigh the benefits of the proposed processing to the controller, consumer and other stakeholders against potential harms to the rights of the consumer. The assessment should also take into account the possibility of using de-identified data and reasonable consumer expectations.

Data Security and Privacy Program Obligations: The Information Protection Act takes a prescriptive approach to data security and privacy risk management. As with other privacy laws, controllers are required to establish, implement and maintain administrative, technical, and physical safeguards to protect the security of the data in their possession. Rather than giving discretion to the controller, the Information Protection Act mandates that controllers must implement a data security program in accordance with the U.S. National Institute of Standards and Technology's Privacy Framework (the NIST Privacy Framework). The NIST Privacy Framework is a voluntary tool designed to help organizations identify and manage privacy risk. The Information Protection Act marks the first instance of a state law requiring at least partial conformance with the NIST Privacy Framework. Failure to maintain a compliant privacy program may also be considered an unfair and deceptive act under Tennessee's consumer protection statute but. establishing and maintaining a compliant privacy program will constitute an affirmative defense. Interestingly, the Information Protection Act also acknowledges that certifications pursuant to the Asia Pacific Economic Cooperation's Cross Border Privacy Rules and Privacy Recognition for Processors systems can also help to establish an affirmative defense to claims.

Enforcement: Like the Montana statute, the Information Protection Act doesn't contemplate private enforcement and allows for a 60-day cure period. Following the cure period, the attorney general may bring an enforcement action seeking declaratory and injunctive relief, attorney's fees and investigative costs, and civil penalties up to USD 7,500 per violation.

Key takeaways

Although the Montana Consumer Data Privacy Act and Tennessee Information Protection Act continue 2023's trend of state privacy legislation and in many respects closely resemble laws already on the books, they each contain unique features of which businesses should take note. The Montana law's requirement that controllers acknowledge opt out preference signals may demand coordination across a range of business units. Likewise, the establishment of a NIST-compliant privacy program mandated by the Tennessee Information Protection Act will require adoption across the whole enterprise.

As a first step, organizations should take careful note of the data-volume of the new laws, which differ in key respects from prevailing privacy legislation, and should undertake data mapping exercises to determine whether the laws apply to them. As always, businesses should also continue to monitor developments as other privacy bills wend their way through the legislative process and determine the requirements of new laws as they relate to their respective businesses.

Should you have questions about this or other data privacy issues, reach out to any of the Baker McKenzie attorneys listed in this alert.

Contact Us

Cynthia J. Cole
Partner
cynthia.cole@bakermckenzie.com

Helena J. Engfeldt
Partner
helena.engfeldt@bakermckenzie.com

Jonathan Tam
Partner
jonathan.tam@bakermckenzie.com