CLIENT ALERTS & INSIGHTS

Montana and Tennessee Join the Fray Enacting Omnibus Data Protection Laws as U.S. State Data Protections Pick Up Pace

MAY 1, 2023

Montana and Tennessee are the latest states to pass data protection laws under a “controller” and “processor” model as 2023 is proving to be a year of Privacy and Security overhaul.

With 2023 showing no signs of slowing down on the data privacy and security front, two new states, Montana and Tennessee, join an existing seven by passing broad, omnibus data protection laws.

Just in the last week, Montana’s state legislature passed the Montana Consumer Privacy Act (the “Montana Law”) and Tennessee’s state legislature passed the Tennessee Information Protection Act (the “Tennessee Law”). Montana and Tennessee now join California, Colorado, Connecticut, Indiana, Iowa, Utah, and Virginia in enacting broadly applicable data privacy and data security requirements on businesses.

California and Virginia’s data protection laws are already in effect, with California delaying enforcement until July 2023. Colorado, Connecticut, and Utah’s data protection laws will come into effect over the course of 2023 as more and more businesses in the U.S. becomes subject to one or more data protection laws. Iowa more recently passed their data protection law last month and it will go into effect January 1, 2025.

Indiana’s data protection law provides a long runway for in-scope entities to come into compliance as the effective date of the Indiana Law is January 1, 2026.

Despite later passage through their applicable state legislatures, the Montana Law and Tennessee Laws come into effect **before** some already existing data protection laws. The Montana Law is effective as of October 1, 2024, and the Tennessee Law is effective July 1, 2024.

Prior to 2021, California was the only U.S. state with a comprehensive data protection law.

Now, there are 9 and 2023 will likely continue to see more states enter the data protection foray so as not to be left behind from the wave of data protection legislation. Below, please find more information on the timing for when each state has data protection laws coming into effect and what businesses will be subject to the data protection laws of a given state.



Scope and Applicability of U.S. State Data Protection Laws

All states set forth a prerequisite that only a business that operates or does business in the specific state is subject to the law. But it is not that simple. To be subject to the applicable state laws, the "do business in the state" prerequisite must be met, but a business must also meet certain "triggers".

There are generally three triggers that could bring a business into the scope of a U.S. State's data protection law: (1) annual gross revenue (not just the revenue derived out of the applicable state); (2) the total collection of personal information from consumers in the applicable state; or (3) the collection and sale of the state's consumers' personal information.

State	Annual Gross Revenue (Aggregate / Worldwide)	Processing of Personal Information (Applicable State Residents)	Sale of Pe (Applicab
California	OVER $25 million	Buying, selling, or sharing 100,000 or more consumers' personal information	50% of gr from selli informati
Colorado	N/A	Processing 100,000 or more consumers' personal information	Receiving consumer controllin 25,000 co informati
Virginia	N/A	Processing 100,000 or more consumers' personal information	Deriving 5 revenue (personal i or process consumer
Connecticut	N/A	Processed 100,000 or more consumer' personal information	Deriving 2 revenue (personal i or process consumer
Utah	**REQUIREMENT:** $25 million or more	Processing 100,000 or more consumers' personal information	Deriving 5 revenue (personal i or process consumer
Iowa	N/A	Processing 100,000 or more	Deriving 5

As the above table indicates, each state has taken a slightly different approach. California arguably has the broadest reach in that **any** business that records an annual gross revenue of over $25 million is subject to the CPRA. Although Montana's lower threshold of processing 50,000 consumers' personal information (in contrast to the 100,000 threshold most states have adopted) might have a broad reach as well.

It is also important to note a big difference between California and the other 8 U.S. states-California includes employee, job applicant, contractor, and business-to-business personal information in the scope of the law. The other 8 U.S. states all include broad exclusions that exempt out the forgoing employee and business-to-business personal information categories.

Utah is still arguably the narrowest in scope in that on top of the "do business in the state" threshold requirement, Utah also requires a prerequisite that the business have an annual gross revenue of $25 million or more. Then, assuming the first two prerequisites are met, a business must meet one of the two collection or sale of personal information triggers.

Montana Data Protection Law Privacy Rights

Under the Montana Law, consumers will having the following rights: (1) to confirm whether a business is processing the consumer's personal information, (2) to correct the personal information a business holds about them; (3) to have their personal information deleted; (4) to receive a copy of the personal information held about them in a portable and usable form (data portability); (5) to opt-out of the sale of their personal information; (6) to opt-out of cross-contextual behavioral targeted advertising; and (7) to opt-out of profiling through solely automated means in furtherance of decisions with legal or similar effect (e.g., employment, education, criminal justice, etc.).

The Montana Law defines "sale" as the exchange of personal information for monetary **or other** purposes-which aligns with California's broad approach to sale including more than data brokers.

Additionally, in line with other new state laws (all except California)-Montana requires businesses to give consumers the right to appeal that businesses denial of a data privacy right request.

For sensitive personal information, the Montana Law requires opt-in consent before a business can collect and process sensitive personal information, instead of merely requiring the provision of an opt-out right such is the case under the California and Utah data protection laws. The Montana Law defines "sensitive personal information" as any category of data identifying: (1) race, ethnicity, or religion; (2) mental or physical health diagnosis; (3) sexual orientation; (4) citizenship or immigration status; (5) genetic or biometric data processed with the purpose of identifying an individual; (6) the personal information of a child (younger than 13); or (7) a person's precise geolocation (within a radius of 1,750 feet).

Tennessee Data Protection Law Privacy Rights

Under the Tennessee Law, consumers will having the following rights: (1) to confirm whether a business is processing the consumer's personal information, (2) to correct the personal information a business holds about them; (3) to have their personal information deleted; (4) to receive a copy of the personal information held about them in a portable and usable form (data portability); (5) to opt-out of the sale of their personal information; (6) to opt-out of cross-contextual behavioral targeted advertising; and (7) to opt-out of profiling through solely automated means in furtherance of decisions with legal or similar effect (e.g., employment, education, criminal justice, etc.);

Additionally, where a business sells their personal information, individuals have the right to obtain a specific disclosure of (i) the categories of personal information sold about the individual; (ii) categories of third parties which the information was sold to (by category of personal information sold); and (iii) the categories of their personal information disclosed for a business purpose.

The Tennessee Law defines "sale" as the exchange of personal information for monetary **or other** purposes-which aligns with California's broad approach to sale including more than data brokers.

Similar to the Montana Law and other recent state data protection laws, the Tennessee Law requires businesses to allow individuals the ability to appeal any denial of their exercise of any data privacy request.

Instead of merely requiring the provision of a right opt-out such is the case under the California and Utah data protection laws, the Tennessee Law requires businesses to obtain prior opt-in consent before processing an individual's sensitive personal information. The Tennessee Law defines "sensitive personal information" as any category of data identifying: (1) race, ethnicity, or religion; (2) mental or physical health diagnosis; (3) sexual orientation; (4) citizenship or immigration status; (5) genetic or biometric data processed with the purpose of identifying an individual; (6) the personal information of a child (younger than 13); or (7) a person's precise geolocation (within a radius of 1,750 feet).

Montana Data Protection Law Enforcement

The Montana Law does not provide individuals with a private right of action against businesses that violate the Montana Law.

Instead of a private right of action, the Montana state attorney general will have exclusive enforcement authority. Prior to any enforcement action, the State Attorney General is required to provide the business a 60 day notice allowing the business 60 days to cure the alleged violation. It is only if the alleged violation is not cured within such 60 day period that the State Attorney General can bring an enforcement action.

Tennessee Data Protection Law Enforcement

In line with the new U.S. state data protection laws, the Tennessee Law does not provide individuals with a private right of action against businesses that violate the Tennessee Law.

Instead of a private right of action, the Tennessee State Attorney General will have exclusive enforcement authority. Prior to any enforcement action, the State Attorney General is required to provide the business a 60 day notice allowing the business 60 days to cure the alleged violation. It is

only if the alleged violation is not cured within such 60 day period that the state attorney general can bring an enforcement action.

Unique to the Tennessee Law that does not exist in the other 8 U.S. state data protection laws is a safe harbor for businesses whose privacy compliance program conforms to the National Institute of Standards and Technology ("NIST") privacy frameworks title "A Tool for Improving Privacy through Enterprise Risk Management Version 1.0" or such successor or updated framework as might be promulgated by NIST from time to time. Businesses that conform a data protection compliance program to the NIST privacy framework and that regularly review their program and update it as necessary have an affirmative defense to any claims for violations of the Tennessee Law.

Conclusion

In 2022, the federal government again failed to seriously consider an omnibus data protection law that would preempt the increasing number of state data protection laws; and it is unlikely the federal government will implement such a federal law anytime soon.

Meanwhile, states will continue to enter the fray of comprehensive data protection laws. While those laws will undoubtably cover similar concepts-they will all present different and important nuances that will require detailed reviews of data protection compliance programs. This has proved true in 2021 and 2022 with California, Colorado, Connecticut, Utah, and Virginia; and now in 2023 with Iowa, Indiana, Montana, and Tennessee.

As more states pass comprehensive data protection laws and such laws come into effect, more and more business will need to build out substantive, data protection compliance programs.

Those programs will need to adaptable-as one business could be subject to multiple state laws and therefore must adapt to the nuanced differences-and will need to account for the different aspects of comprehensive data protection laws, such as (1) substantive privacy policies and notices; (2) consumer privacy right request policies and procedures; (3) reasonable, adequate technical, organizational, and physical security measures; (4) vendor and contract management programs to flow through required contractual provisions when engaging data processors and service providers; and (5) regular audit procedures and programs.

The above list is not exhaustive of all a business would need to do under the applicable U.S. State laws; but it provides an example of the different requirements comprehensive data protection laws set forth-and the time it will take for business to build out compliant programs.

Businesses that have not previously dealt with comprehensive data protection law compliance will need to invest a significant amount of time in developing the required policies and procedures. Additionally, even if businesses have previously dealt with other-or former versions of-comprehensive data protection laws, they will need to conduct comprehensive reviews to account for specific nuances and difference in the laws.

As more states continue to implement their own variations of data protection laws and business juggle the various requirements, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.