DORSEY
DORSEY+WHITNEY LLP

Leaning Toward Commonality: States Enact New Comprehensive Consumer Data Privacy Laws

June 14, 2023 – The TMCA
by Dustin Berger

The year 2023 will likely go down in history as a major inflection point in the enactment of comprehensive consumer data privacy laws in the United States. At the beginning of the year, only five states (California, Virginia, Colorado, Utah, and Connecticut) had enacted comprehensive consumer data privacy laws. And, of these, only the California and Virginia laws are currently in effect. The privacy laws in Connecticut and Colorado go into effect on July 1, 2023, and Utah's law becomes enforceable on December 31, 2023.

Related People

- Dustin Berger

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

Recently, however, the states of Indiana, Iowa, Tennessee, and Montana have also enacted new state consumer data privacy laws. In addition, state legislatures in Florida and Texas have passed bills to enact consumer data privacy laws; the governors of these states are widely expected to sign these bills into law. Most privacy professionals anticipate that many of the remaining states will also enact privacy laws in the next few years. It is likely that, barring preemptive federal law-making, most or all of the remaining states will eventually enact privacy laws of their own. (The state of Washington also recently enacted a landmark privacy law specific to consumer health data this year that

also has some overlap with these comprehensive consumer data privacy laws.)

Many businesses and other organizations have expressed concern about the compliance burdens of dealing with these emerging privacy laws, particularly since they can be subject to the laws of each jurisdiction in which they do business. Nevertheless, there is significant commonality among the laws that have passed so far. It is reasonable to assume that laws enacted in the future will continue to have these comment elements. By focusing on these common elements, businesses can design their privacy program with the confidence that it will be well positioned for the future. These common elements include the following features:

- *Applicability thresholds*. Although the specific thresholds vary, each of the state laws has applicability requirements that exempt many small and medium businesses that are not heavily involved in personal data collection or sales. Iowa and Indiana's laws are typical in this respect. For either of those states' laws to apply, the business or organization must process the personal data of 100,000 or more residents of the state or, if the business derives 50% or more of its gross revenue from the sale of personal data, process the data of 25,000 or more residents of the state. And, except in Colorado, non-profit organizations are exempt from compliance. Each law also has broad exemptions for organizations or personal data that is already protected under existing federal sectoral privacy laws like the Health Information Portability and Accounting Act (HIPAA) and the Gramm Leach Bliley Act (GLBA).
- *Exclusion of personal data of employees, applicants, and former employees*. With the exception of California, no state has applied its consumer data privacy law to individuals in their role as members of their employers' workforces. Emergency contact information and personal data used for benefit administration is often also exempted from the laws' requirements.
- *Data subject rights*. All states provide individuals in the state with rights relating to their personal data. These rights generally include the right to deletion of personal data, the right to correct inaccurate data, the right to know what data the business holds regarding the individual, and the right to receive a portable copy of the individual's personal data. Most states also give individuals the right to opt out of the selling of their personal data or sharing of their personal data for behavioral advertising. A few states even give individuals the right to opt-out of certain kinds of processing of consumer data.
- *Privacy notice requirements*. Each of the states has requirements for privacy-related disclosures. Every state privacy law currently enacted requires businesses to state the categories of personal data that they collect and the purposes for the collection. Some states also require additional disclosures about the sharing and selling of personal data and place limits on the processing of personal data for purposes in excess of what was disclosed at the time of collection. And, all states require that privacy notices (often called privacy policies) explain the rights individuals have regarding their personal data.
- *Sensitive data rules.* Many states designate a category of personal data as "sensitive data" to reflect the higher risk of harm that could be associated with its use. Montana's definition is typical and defines sensitive data as including: "(a) 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; (b) the processing of genetic or biometric data for the purpose of uniquely identifying an individual; (c) personal data collected from a known child; or (d) precise geolocation data." Some states require consent from the individual to process sensitive data, while others allow individuals to opt out of the processing of

sensitive data.

- *Security requirements.* All of the state privacy laws require organizations to protect personal data with reasonable information security safeguards.
- *Data protection agreements*. Most of the state privacy laws require businesses that engage processors (*e.*, third parties that process personal data on their behalf) to have a contract with the processor that contains specific requirements, such as instructions for the personal data processing, the nature and purpose of the processing, the type of data subject to processing, the duration of the processing, return or deletion of the personal data at the end of the relationship, and assisting in demonstrating compliance with the law.
- *Data protection assessments*. Many of the state privacy laws have provisions that require businesses that engage in processing of personal data involving a high risk to the data subject to thoroughly analyze the processing, weigh the risks and benefits, consider ways to mitigate risks, and possibly consider alternatives and safeguards. (This assessment is sometimes also called a data protection impact assessment or privacy impact assessment.) Most of these laws consider the processing of personal data for targeted advertising or selling personal data to be activities for which an assessment is required. Similarly, the processing of sensitive data requires an assessment in many states.
- *No Private Enforcement*. In general, state privacy laws allow only governmental enforcement, and do not grant individuals a private right of action to sue for damages. California is the sole exception, but even in California, an individual can sue only if the individual was a victim of a data breach.
- *Cure periods*. Many laws provide that, prior to enforcement, a business is entitled to notice of an alleged problem and a right to cure the violation within a certain specified period.
- *Civil penalties*. All of the laws provide for civil penalties, often of $7,500 or more per violation.

The following table describes how Iowa, Indiana, and Tennessee have addressed these common elements.

Feature	**Iowa**	**Indiana**	**Tennessee**	**Montana**
Applicability threshold	Process personal data of 100,000 residents or Process personal data of 25,000 residents and receive 50% or more of gross revenue from sale of personal data	Process personal data of 100,000 residents or Process personal data of 25,000 residents and receive 50% or more of gross revenue from sale of personal data	Have $25 million or more worldwide annual gross revenue and process personal data of 175,000 residents or Process personal data of 25,000 residents and receive 50%	Process personal data of 50,000 residents or Process personal data of 25,000 residents and receive 25% or more of gross revenue from sale of personal data

			or more of gross revenue from sale of personal data	
Data subject opt-out rights	Sale of personal data, targeted advertising, sensitive data processing	Targeted advertising, sale of personal data, profiling with significant consequences	Sale of personal data, targeted advertising	Targeted advertising, sale of personal data, profiling with significant consequences
Other data subject rights	Confirm processing, deletion, receive a copy, appeal	Confirm processing, correction, deletion, receive a copy, appeal	Confirm processing, correction, deletion, receive a copy, appeal, request information about data sales	Confirm processing, correction, deletion, receive a copy
Exclusions for data covered by HIPAA and GLBA and for institutions of higher education	Yes	Yes	Yes	Yes
Requirement for a privacy notice required that is organized by categories and purposes and including information on rights	Yes, and it must also list categories of personal data shared with third parties and categories of third parties	Yes, and it must also list categories of personal data shared with third parties and categories of third parties	Yes	Yes, and it must also list categories of personal data shared with third parties and categories of third parties
Privacy notice serves as a processing limitation	No	Yes	Yes	Yes

(i.e. the law limits processing personal data for purposes other than those described at collection)				
Data protection assessments required	No	Yes	Yes	Yes
Reasonable data security requirement	Yes	Yes	Yes	Yes
Data processing agreement requirements	Yes	Yes	Yes	Yes
Private right of action	No	No	No	No
Right to cure	Yes, 90 days	Yes, 30 days	Yes, 60 days	Yes, 60 days, but it expires on April 1, 2026.
Effective date	Jan. 1, 2025	Jan. 1, 2026	July 1, 2024	Oct. 1, 2024
Civil penalty	Up to $7,500 per violation	Up to $7,500 per violation	Up to $15,000 per violation	Yes, with no explicit cap

By building a privacy compliance program that can effectively deal with these common elements, business and other organizations can feel confident that their program will also satisfy many of the elements that will be present in future state data privacy laws. Here at the TMCA, we will continue to keep stakeholders updated on further developments in the fast-moving area of consumer privacy legislation.