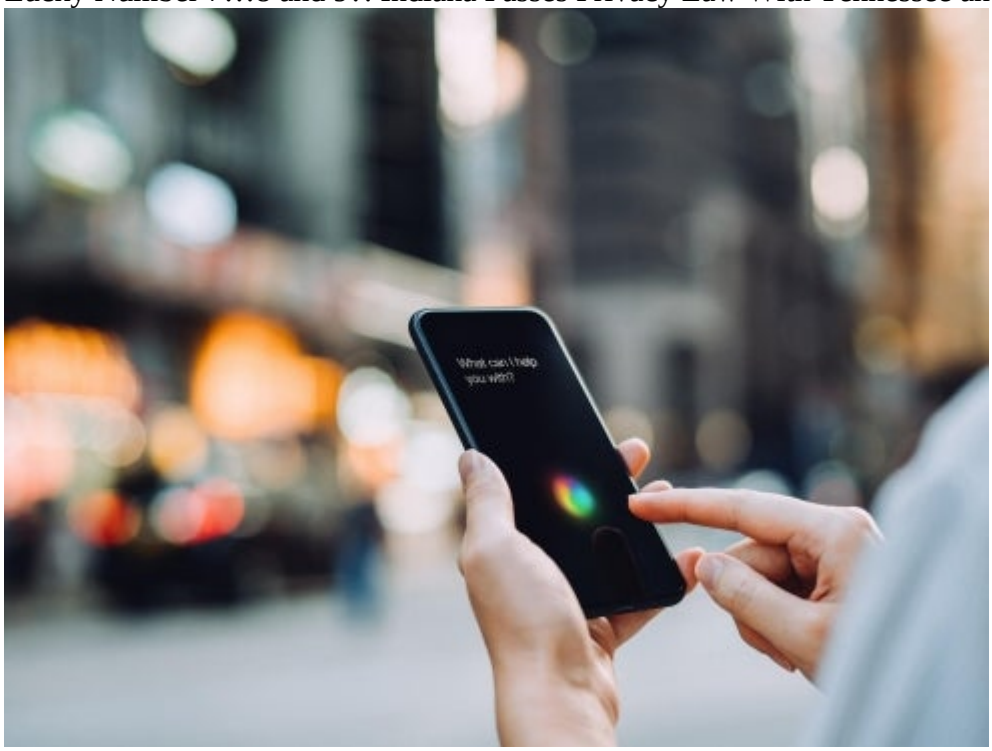
Blogs
May 02, 2023
Lucky Number 7…8 and 9?: Indiana Passes Privacy Law With Tennessee and Montana Hot on Its Heels



Indiana Governor Eric Holcomb signed Senate Bill 5 on May 1 (effective January 1, 2026), making Indiana the seventh state to offer comprehensive privacy protections. Indiana's new law appears to closely track Virginia's omnibus privacy law. The law will apply to a person that conducts business in Indiana or produces products or services targeted to Indiana residents, and that meets either of the following requirements in a calendar year: (1) controls or processes the personal data of 100,000 consumers (defined as residents of Indiana "acting only for a personal, family, or household purpose"); or (2) controls or processes personal data of at least 25,000 consumers with more than 50% of annual gross revenue derived from the sale of personal data.

Similarly, both Tennessee and Montana appear to be imminently close to enacting their own state comprehensive privacy bills. The Tennessee and Montana legislatures each passed their own state bills on April 21, 2023, and each bill is expected to be signed into law by the respective governor soon.

Below, we look at some of the key similarities and differences between the new Indiana privacy law compared with the other six state omnibus privacy laws. We also highlight the key provisions of the Tennessee and Montana bills that are expected to be signed into law soon.

Across the Board: Key Similarities in Indiana

Like the privacy laws in California, Colorado, Connecticut, Iowa, Utah, and Virginia, the Indiana law establishes consumer privacy rights. These include the rights of deletion, portability, non-discrimination, and the right to opt out of processing of the consumer's personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

Along these lines, the Indiana law imposes business requirements that generally align with those in the other states. For example, businesses are required to conduct and document data protection impact assessments

(DPIAs) for certain processing activities, including for the purpose of targeted advertising, the sale of personal data, and the processing of sensitive data. Like many of the other states, Indiana requires businesses to utilize privacy by design principles like purpose specification and data minimization. Indiana does not offer consumers a private right of action. Instead, the attorney general has the exclusive right to enforce the law and has the authority to initiate actions, seeking civil penalties up to $7,500 per violation. Unlike states like California and Connecticut that contain sunset provisions, in Indiana the attorney general must permanently give businesses 30 days to cure any alleged violations.

The House Edge: Key Differences in Indiana

Unlike California's privacy law, the Indiana law does not apply to individuals acting in a commercial or employment context. While Indiana offers the right to correct inaccuracies, this right is uniquely limited to "inaccuracies in the consumer's personal data that the consumer previously provided to a controller." Like the other states, Indiana offers consumers the right to request access to their personal data. However, the law allows controllers to choose whether to provide consumers with a copy of their personal data, or alternatively, a representative summary of this data. Controllers are required to consider the nature of the personal data and the processing purposes when determining how to respond to an access request.

Indiana's is the first of the state privacy laws to offer an exception allowing licensed riverboat casino owners to use state gaming commission-approved facial recognition programs on their property without it constituting a violation of the privacy law. The attorney general has permissive authority to maintain a list of resources for controllers on its website, which may include sample privacy notices and disclosures, to help controllers with compliance.

Finally, the Indiana law goes slightly further than other laws and offers more guidance surrounding what constitutes publicly available information, noting that a business has a reasonable basis to believe such information is lawfully made available when it is provided (1) to the general public through widely distributed media, (2) by the consumer to whom the information pertains, or (3) by the person to whom the consumer has disclosed the information, unless the consumer restricted the information to a specific audience.

Highlights of the Montana and Tennessee Bills

The Tennessee Information Protection Act (TIPA) and Montana Consumer Data Privacy Act (MCDPA) appear to be next in line for passage. Below we highlight some of the most critical provisions in each bill.

Tennessee Information Protection Act

For those familiar with the Virginia Consumer Data Protection Act (VCDPA), this state law will appear refreshingly similar. If signed by Governor Bill Lee, TIPA will go into effect starting July 1, 2024, setting into place a series of consumer rights and business obligations generally in line with Virginia's law.

However, TIPA would carry with it some key differences that we highlight here. TIPA defines consumers more narrowly than other states, limiting consumers to "a resident of [Tennessee] acting only in a personal context." Unlike Virginia, TIPA defines a "sale" of personal information as the exchange of personal information for "monetary or other valuable consideration," thus broadening what constitutes a sale for businesses as compared to Virginia, which only is concerned with the exchange of personal information for monetary consideration.

Most notably, TIPA's enforcement provisions represent a shift from Virginia's. Similar to Virginia, there would be no private right of action and enforcement authority would rest entirely with the attorney general. Yet unlike

Virginia's, TIPA's penalty of $15,000 for each violation would be a marked, two-fold increase over Virginia's, although this is accompanied with a 60-day cure period that does not sunset–twice as long as Virginia's 30-day cure period.

Montana Consumer Data Privacy Act

If enacted by Governor Greg Gianforte, the MCDPA would become effective on October 1, 2024, putting enforcement by Montana ahead of enforcement in the states of Iowa or Indiana. The MCDPA would be the first state law to cut the scoping threshold requirements and would apply to businesses that (1) control or process personal data of 50,000 Montana consumers or (2) control or process personal data of at least 25,000 consumers and derive more than 25% of gross revenue from the sale of personal data (instead of the typical 100,000 consumers or 50% thresholds found in other states). Additionally, Montana is unique in including provisions applicable to teens, whereby teens that are "at least 13 years of age but younger than 16 years of age" would need to consent to sales of their personal data and for targeted advertising.

With regard to opt-out rights, the MCDPA follows the trend of some states in granting consumers the ability to exercise opt-out rights using a universal technological mechanism, like a browser extension or "global device setting." Montana differentiates itself from other states, though, as it allows consumers' opt-out rights to extend to pseudonymized data unless the controller can demonstrate that information needed to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information. Finally, enforcement would be carried out exclusively by the attorney general and there is no private right of action, but the MCDPA would offer a 60-day cure provision that would expire on April 1, 2026.

* * * * *

While it is not expected that the Indiana law or the Tennessee or Montana bills will significantly increase or complicate the compliance burden for companies that are already addressing their obligations under the other state privacy laws, companies should review their privacy practices to ensure they meet specific state privacy law requirements as they come into effect. Additional states may pass omnibus privacy laws that diverge from the status quo, and we will continue to monitor developments and publish updates as the legislative environment evolves.

Authors

Explore more in

Privacy Litigation Privacy & Security