Tennessee Information Protection Act Approved by Lawmakers

On April 21, Tennessee lawmakers approved and sent to Governor Bill Lee for signature, the Tennessee Information Protection Act (TIPA), one of nine different state consumer privacy laws that are generally considered to be comprehensive. TIPA's passage is part of a growing flood of state privacy laws across the United States, with four having passed this spring along with other privacy laws impacting specific types of data. TIPA does not take effect for over two years, with a current effective date of July 1, 2025.

TIPA Applicability

TIPA applies to entities (known as controllers) that conduct business in Tennessee and produce products or services that are targeted to residents of Tennessee, exceed more than $25,000,000 in "revenue," *and*:

- During a calendar year, control or process the personal information of 175,000 or more Tennessee residents (consumers); or
- Control or process the personal information of at least 25,000 consumers *and* derive more than 50% of gross revenue from the sale of personal information.

TIPA also applies to vendors and others (known as processors) that process personal information on behalf of a controller. TIPA does not define "revenue" but, like California and Utah, we believe that the term will be defined to mean annual gross revenue on a worldwide basis.

TIPA defines a "consumer" as a natural person who is a resident of Tennessee acting in a personal context. This means that employees and business-to-business (B2B) contacts are expressly excluded from the definition of "consumer."

TIPA Rights

Under TIPA, consumers are granted the right to do all of the following:

- **Access** their personal information (including a right to confirm whether a controller is processing their personal information).
- **Delete** personal information provided by or obtained about them.
- **Obtain a copy** of the consumer's personal information in a portable format, but limited to data the consumer previously provided.
- **Correct inaccuracies** in their personal information, but limited to data the consumer previously provided.
- **Appeal** any denial of a consumer request relating to the above rights.

Also, the controller must give the consumer the ability to **opt out** of the following:

- Profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.
- Targeted advertising.

- The sale of personal information.

TIPA expressly states that if any of the data is "pseudonymous" data (i.e., data in which any identifiers are kept separately and are subject to controls to prevent the controller from accessing those identifiers) or de-identified data (i.e., data that cannot be attributed to a specific natural person or device linked to a person), then opt-out rights do not apply.

TIPA Responsibilities of Controllers and Processors

As with other states' laws, controllers must limit the purpose of processing personal information to that which is reasonably necessary and proportional; take steps to implement reasonable technical and organizational measures to protect the security of personal information; avoid unlawful discrimination against consumers for exercising their rights; be transparent in their reasonably accessible, clear and meaningful privacy notice; and ensure contracts control relationships with their processors. A processor shall adhere to the processing instructions of a controller and assist the controller in meeting its obligations to respond to consumer rights requests and conduct a data protection assessment by providing necessary information.

Additionally, controllers must obtain the consumer's consent to process sensitive data or, in the case of the processing of sensitive data concerning a known child, process the data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) and its implementing regulations.

As noted above, there is a data protection assessment requirement for all controllers. These assessments must identify and weigh the benefits of a particular use that may flow to the controller, consumer, other stakeholders, and the public versus any potential risks to the rights of the consumer. The assessment must consider the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal information will be processed. Notably, this requirement will apply to processing activities created or generated on or after July 1, 2024, and are not retroactive. Processors are required to reasonably assist controllers with undertaking such assessments.

TIPA Enforcement and Affirmative Defense for Compliance with NIST

Under TIPA, the Tennessee Attorney General (AG) has exclusive authority to enforce any violation of the law, and there is an express provision disclaiming any private right of action. Prior to being penalized, controllers and processors have a 60-day right–to-cure period in which they can provide an express written statement that the alleged violations have been cured and that no further violations will occur. Notably, this cure period does not sunset. If the controller or processor fails to cure, the AG may impose a civil penalty of up to $7,500 for each violation.

In the event of an allegation of violation of TIPA, a controller or processor has an affirmative defense if it creates, maintains, and complies with a written privacy program that conforms to the National Institute of Standards and Technology (NIST) privacy framework entitled "A Tool for Improving Privacy through Enterprise Risk Management Version 1.0" or "other documented policies, standards, and procedures designed to safeguard consumer privacy." If the NIST or a comparable privacy framework publishes a subsequent revision to its privacy framework, a controller or processor shall reasonably conform its privacy program to the revised framework no later than two years after the publication date stated in the subsequent version.

If you have questions about TIPA or other state or federal privacy laws and how they could affect you or your business, please contact the authors.