Tennessee's Information Protection Act – What Businesses Should Know.

On May 11, 2023, the Tennessee Information Protection Act ("TIPA") was signed into law effective on July 1, 2025. In doing so, Tennessee has joined the patchwork of U.S. consumer privacy laws following the enactment of the California Consumer Privacy Act. Here's what businesses should know.

Who's Covered.

TIPA applies to entities conducting business in Tennessee, and any business that offers products or services targeted to Tennessee residents (called "controllers"), that exceeds $25 million in annual revenue and either:

(i) Controls personal information of at least 175,000 Tennessee residents; or
(ii) Controls personal information of at least 25,000 Tennessee residents while deriving more than 50% of its gross revenue from the sale of personal information.

The law includes common entity exemptions, such as government entities, financial institutions regulated by the Gramm-Leach-Bliley Act, insurance companies, covered entities and business associates regulated by the Health Insurance Portability and Accountability Act ("HIPAA"), nonprofit organizations, and higher education institutions.

TIPA also provides data-specific exemptions, including HR data and information governed by the Fair Credit Reporting Act, HIPAA, Health Information Technology for Economic and Clinical Health Act, Family Educational Rights and Privacy Act, Driver's Privacy Protection Act, Farm Credit Act, and Controlled Substances Act.

The definition of a consumer[1] excludes individuals acting in an employment or business to business (B2B) context. De-identified or pseudonymous data is generally exempt from TIPA's provisions.

Consumer Rights.

Controllers are required to comply with consumer requests to know and access the consumer's personal information and to correct, delete, and disclose the categories of information about the consumer that have been sold. Consumers may request to opt out of a controller (i) selling their personal information, (ii) processing personal information for targeted advertising, and (iii) profiling consumers. The sale of information is defined similar to the majority of U.S. consumer privacy laws, i.e., the exchange of personal information for valuable monetary consideration.

Upon receipt of a consumer request, a controller is required to comply within 45 days unless the controller notifies the consumer that it requires an additional 45 days along with the reason for the delay.

If a controller declines to satisfy a consumer request, the controller is required to disclose the justification and instruct the consumer on how to appeal the decision within 45 days of receipt of the request. A controller must furnish a response to an appeal within 60 days, and in the event an appeal is denied, the controller is obligated to provide the consumer with a method for contacting the attorney general's office.

Business Requirements.

[1] TIPA defines "consumer" as a natural person who is a resident of Tennessee "acting only in a personal context."

Generally, controllers must (i) obtain consumer consent for processing sensitive data,[2] (ii) implement and maintain reasonable data security practices, (iii) avoid unlawful discrimination, (iv) limit data collection and processing to what is necessary, and (v) provide consumers with a privacy notice. A controller is not required to delete information that it uses as aggregate or de-identified data if the data is not traceable to a specific consumer.

Privacy notices should include: (i) the categories of personal information processed by the controller, (ii) the purpose for processing personal information, (iii) the method by which consumers may exercise their rights, (iv) the categories of personal information that the controller sells to third parties, (v) the categories of third parties to whom the controller sells personal information, and (vi) the right to opt out of the sale of personal information to third parties or processing personal information for targeted advertising.

Contracts with service providers (called "processors") must contain certain key terms, including a duty of confidentiality, deleting or returning personal information upon request, making available information to demonstrate the processor's compliance with obligations, allowing a reasonable assessment by the controller or controller's designated assessor or, alternatively, arranging for a qualified, independent assessor to conduct an assessment of the processor's policies and technical/organizational measures in support of its obligations using an appropriate and accepted control standard or framework and assessment procedure. Such contracts must also outline specific data processing procedures.

Data Protection Assessments.

TIPA requires controllers to conduct and document a data protection assessment when processing personal information for purposes of (i) targeted advertising,[3] (ii) processing sensitive data, (iii) selling personal information, or (iv) processing personal information for profiling when such processing presents a reasonably foreseeable or heightened risk of harm to consumers[4]. Data protection assessments conducted in compliance with other state law may comply with TIPA if the assessments have a similar scope and effect. Data protection assessment requirements will apply to processing activities generated or created on or after July 1, 2024.

How It's Enforced.

TIPA provides that the Tennessee attorney general (AG) shall enforce it, including the right to investigate any entity believed to be engaging in a violation. If the entity fails to cure the violation within 60 days, the AG may bring an action for declaratory, injunctive, and monetary relief, including $7,500 in civil penalties per violation. If a controller willfully or knowingly violates TIPA, the AG may

[2] Sensitive data includes: (i) personal information revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status, (ii) the processing of biometric or genetic data, (iii) personal information collected from a known child younger than thirteen years of age, or (iv) precise geolocation data (GPS that directly identifies the specific location of a person with precision and accuracy within a radius of 1,750 ft.).

[3] Targeted advertising means displaying advertisements that is based on personal information obtained from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests.

[4] TIPA defines the risk of harm to consumers as (A) unfair, deceptive or disparate treatment; (B) financial, physical or reputational injury; (C) physical or intrusion upon the private affairs of consumers where the intrusion would be offensive to a reasonable person; or (D) other substantial injury.

seek treble damages. The AG may recover reasonable expenses incurred in investigating and preparing a case, including attorney's fees. There is no private right of action under TIPA.

First-Of-Its Kind Affirmative Defense.

Unlike other U.S. consumer privacy laws, TIPA includes a provision allowing controllers charged with a violation to raise an affirmative defense if they create, maintain, and comply with a written privacy program that conforms to the National Institute of Standards and Technology's ("NIST") privacy framework.

Whether a controller's privacy framework reasonably conforms to the NIST privacy framework depends on the following factors:

(i) The size and complexity of the controller or processor's business;
(ii) The nature and scope of the activities of the controller or processor;
(iii) The sensitivity of the personal information processed;
(iv) The cost and availability of tools to improve privacy protections and data governance; and
(v) Compliance with a comparable state or federal law.

It is becoming increasingly more difficult for businesses to implement a comprehensive U.S. privacy program with the patchwork of state laws. The differences in TIPA make it imperative that businesses become familiar with its requirements to maintain their compliance.

--Melody McAnally

69474851.v2