



Privacy & Cybersecurity Update

May 2023

Data Privacy Update: Several U.S. States Enact Privacy Legislation in 2023

In 2023, we have seen several significant developments regarding new data protection laws and regulations in the United States. For example, Iowa and Indiana have recently enacted their own comprehensive consumer privacy laws becoming the sixth and seventh states, respectively, to do so. In addition, Montana and Tennessee's state legislatures have each passed comprehensive privacy laws, which likely will be signed into law. Below is a summary of some of the key issues related to each legal framework, and organizations that collect personal data on their employees, customers, or contractors need to continue to monitor their ever-evolving compliance obligations.

New Privacy Legislation – Iowa, Indiana, Montana, and Tennessee

Iowa. On March 28, 2023, Governor Kim Reynolds signed Iowa's comprehensive data protection bill into law. It applies to entities conducting business in Iowa or targeting consumers in the state that either (i) control or process the personal data of at least 100,000 residents or (ii) process the personal data of at least 25,000 consumers and derives over 50% of gross revenue from the sale of personal data. The law only applies to Iowa residents acting in "an individual or household context" and, among many other exemptions, it does not apply to "a natural person acting in a commercial or employment context."

Under its new law, Iowans now have the right to (i) confirm whether a business is processing their personal data, and if so, the right to access such data, (ii) have a business delete their personal data in certain circumstances, and (iii) opt out from having a business sell their personal data. The law

further incorporates other hallmark provisions that have become familiar under similar state laws, such as disclosing its privacy practices, requiring contracts with data processors, and prohibiting discriminatory practices against individuals who exercise their privacy rights.

Importantly, the law does *not* provide consumers with the right to correct their personal data, or expressly provide a right for individuals to request that a business refrain from using their personal information for targeted advertising (which has become a common right in U.S. state data privacy laws). Importantly, however, the law does mandate that if a business engages in targeted advertising, it must "clearly and conspicuously disclose such activity, as well as the manner in which a consumer may exercise the right to opt out of such activity."

The Iowa privacy law does not grant individuals a private right to action. Iowa's attorney general has exclusive enforcement authority, which includes the power to impose monetary penalties of up to \$7,500 per violation. The law takes effect on January 1, 2025.

Indiana. On May 1, 2023, Governor Eric Holcomb signed Senate Bill (SB) 5 into law, which is Indiana's consumer data privacy law. Like Iowa's new law, SB 5 applies to entities conducting business in Indiana or targeting consumers in the state that either (i) control or process the personal data of at least one hundred thousand (100,000) consumers who are Indiana residents or (ii) control or process the personal data of at least 25,000 Indiana residents and derives more than 50% of gross revenue from the sale of personal data. The law has many exemptions, including exemptions

related to personal data collected and used for human resources (HR) purposes.

SB 5 provides individuals with the following privacy rights: (i) the right to confirm whether a covered business is processing their personal data, (ii) the right to correct inaccuracies in their personal data (which is a right not granted in Iowa's law), (iii) the right to have a business delete their personal data, (iv) the right to obtain a copy of their personal data which is in the custody or control of a business, and (v) the right to opt out from having their personal data sold or used for targeted advertising or certain types of profiling.

The Indiana attorney general has exclusive authority to enforce the law; and therefore, there is no privacy right of action for general non-compliance, and the law does not take effect until January 1, 2026.

Montana. On April 21, the Montana Senate formally approved Senate Bill (SB) 384, and Montana's new consumer data protection bill will now be transmitted to Governor Greg Gianforte, and it is anticipated he will sign the bill into law.

SB 384 would apply to entities conducting business in Montana or producing products or services targeting residents in the state and that either: (i) control or process the personal data of at least 50,000 consumers excluding personal data controlled or processed solely to complete a payment transaction or (ii) control or process the personal data of not less than 25,000 consumers and derive more than 25% of gross revenue from the sale of personal data.

SB 384 provides individuals with the right to (i) confirm whether a covered business is processing their personal data, (ii) correct inaccuracies in their personal data, (iii) delete their personal data, and (iv) obtain a copy of personal data previously provided by the consumer to the controller. It also provides residents with the right to opt out of having their personal data sold or used for targeted advertising or certain types of profiling.

Pursuant to SB 394, a consumer may designate an authorized agent by using technology (e.g., internet link,

browser setting, browser extension, or global device setting) to opt out of targeted advertising, profiling, and sale of personal data. The law provides instructions on how covered businesses can receive and respond to these opt-out requests with a compliance date of no later than January 1, 2025.

The Montana attorney general has exclusive authority to enforce the law, which includes a temporary notice-and-cure period for alleged violations. If enacted, SB 384 would take effect on October 1, 2024.

Tennessee. On April 21, the Tennessee Senate formally approved the Tennessee Information Protection Act (TIPA), and it is likely to be signed into law by Governor Bill Lee.

TIPA applies to entities that conduct business in Tennessee or produce products or services that target residents of the state and that either (i) during a calendar year, control or process personal information of at least one hundred thousand (100,000) consumers or (ii) control or process personal information of at least twenty-five thousand (25,000) consumers and derive more than fifty percent (50%) of gross revenue from the sale of personal information.

TIPA provides, with certain exceptions, individuals with the following rights: (i) to confirm whether a controller is processing the consumer's personal information and to access such personal information, (ii) to correct inaccuracies in the consumer's personal information, (iii) to delete personal information provided by or obtained about the consumer, (iv) to obtain a copy of the consumer's personal information that the consumer previously provided to the controller, (v) to opt out of the sale of personal information, and (vi) to request information on the categories of personal information sold or disclosed to third parties by the business, as well as the categories such parties to whom personal information was sold or disclosed.

Importantly, TIPA requires controllers or processors to create, maintain, and comply with a written privacy program that reasonably 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." and modified to conform with subsequent revisions.

The Tennessee attorney general has exclusive authority to enforce the law, and there is no privacy right of action for general non-compliance. If enacted into the law, TIPA will enter into force on July 1, 2024.

Conclusion

The data protection compliance requirements for organizations conducting business in the U.S. continue to multiply, and there are as many as 18 additional privacy bills currently pending in state legislatures. To ensure legal compliance, businesses must remain vigilant in reviewing, tracking, and updating their data protection programs to meet these new and evolving requirements.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky

216.566.5646

202.263.4126

Steve.Stransky@ThompsonHine.com

Certified Information Privacy Professional/Government (CIPP/G)

Certified Information Privacy Professional/United States (CIPP/US)

Thora Knight

212.908.3971

Thora.Knight@ThompsonHine.com

This advisory bulletin may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgment of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions.

© 2023 THOMPSON HINE LLP. ALL RIGHTS RESERVED.