Published on *The National Law Review* https://natlawreview.com

Data Breach Laws on the Books in Every State; Federal Data Breach Law Hangs in the Balance

Article By:

Petrina Hall McDaniel

Keshia Lipscomb

With no central federal data breach law, states have taken the reins, passing an increasing number of laws that require both the protection of citizens' private data and prompt notice of any breach of that privacy. Governors in the last two holdout states, South Dakota and Alabama, recently signed bills to enact laws governing data breaches. Now, all 50 states (plus D.C., Guam, Puerto Rico, and the Virgin Islands) have passed data breach notification laws.

On March 21, 2018, South Dakota enacted Senate Bill No. 62, to be codified as a new section of S.D. Codified Law § 22-40, effective July 1, 2018. The law applies to any person or business "that conducts business in this state, and that owns or licenses computerized personal or protected information of residents." South Dakota's new law is similar to the notification laws in many other states in protecting the disclosure of "personal information" and "protected information." But South Dakota has taken a few unique positions. For instance, South Dakota's law applies only to breaches of "computerized data" and does not extend to information stored in other formats (e.g., on paper). Also notable, South Dakota has adopted a "risk of harm" exception to its general 60-day breach notification requirement, providing that an information holder need not notify residents of a breach if it "reasonably determines that the breach will not likely result in harm to the affected person."

Just a week after South Dakota, Alabama became the final state to enact a data breach notification law. On March 28, 2018, the Alabama legislature unanimously passed SB 318, the Alabama Data Breach Notification Act of 2018, with an effective date of May 1, 2018. Alabama's law applies to any person or entity "that acquires or uses sensitive personally identifying information." Alabama's law goes a step further than many other state data laws in requiring specific measures to protect data privacy. For example, Alabama requires that covered entities "implement and maintain reasonable security measures to protect sensitive personally identifying information," based on the size of the entity, the amount of sensitive personally identifying information maintained by the entity, and the entity's cost in implementing security measures. Alabama's law also requires that a covered entity "conduct a good faith and prompt investigation" of any breach. This includes, at least, assessing the nature and scope of the breach, identifying the potentially affected information, determining whether the information has been acquired and is "reasonably likely to cause substantial harm" to affected individuals, and identifying and implementing measures to restore security.

Just as all states have adopted data breach laws, Congress has taken the initial steps into the realm of data breach laws—to the dismay of state attorneys general currently charged with enforcing these laws. In February 2018, two House Representatives circulated a draft of a proposed Data Acquisition and Technology Accountability and Security Act that would set federal requirements for data privacy and data breach notification—and preempt stronger state data breach laws. As currently drafted, the federal law would trigger liability only if the data breach is "reasonably likely to result in identity theft, fraud, or economic loss."

At present, it appears states fear a federal law regarding data breach will interfere with, rather than enhance, the states' laws. On March 19, 2018, a group of 32 attorneys general joined in writing a letter to the House of Representatives to object to the proposed federal law. The AGs expressed concern with the federal law allowing entities to judge whether to notify consumers and limiting application to breaches of only 5,000 or more consumers. States have generally taken the position that their state laws more comprehensively apply to all data breaches and allow for more consumer-focused enforcement. States continue to refine the scope of their data breach laws, with, for example, Arizona recently expanding its law to apply to the disclosure of certain healthcare data.

It remains to be seen whether Congress will pass a federal data breach law, which many presume is unlikely; in the meantime, businesses must continue to monitor the dynamic patchwork of state data breach laws to ensure compliance.

National Law Review, Volume VIII, Number 120