

Consumer Data Privacy Laws Pose New Mandates in Spate of States



The landscape of consumer data privacy laws in the United States is rapidly evolving, with the number of states implementing comprehensive privacy legislation on the rise. This year alone, the count of states with such laws is expected to nearly double to a total of 10. Iowa, Indiana, and Tennessee have recently joined the list of states enacting privacy laws, while bills in Montana and Florida are awaiting gubernatorial approval. This surge of legislative activity expands on the existing five states that already have comprehensive privacy laws, granting consumers more control over their personal data.

While the new measures generally align with existing state privacy approaches, they feature some specific provisions variations. State lawmakers have been advocating for broad consumer protections through comprehensive privacy laws and narrower privacy proposals, given the absence of a comprehensive federal law on the matter.

Whenever a new state privacy law is enacted, businesses are tasked with assessing its applicability to their operations. David Saunders, a partner at McDermott Will & Emery LLP, explains that companies must determine how the new law differs from existing ones and adjust their practices accordingly. This process can be complex and time-consuming, as each state law has its own unique requirements.

More states will likely contribute to the privacy patchwork by enacting their laws this year. For instance, lawmakers in Texas are currently working on a comprehensive privacy bill after the House and Senate passed separate versions.

Don't wait to take the next step forward in your legal career - submit your resume to LawCrossing today!

The comprehensive laws implemented in these states follow similar frameworks to those previously enacted in Colorado, Connecticut, Virginia, and Utah. Notably, California stands out as the only state to have established a dedicated regulatory agency, the California Privacy Protection Agency, responsible for overseeing its privacy law and issuing relevant regulations.

These laws primarily target companies that conduct business and collect data from residents within each state. However, the thresholds for determining which companies fall under the new requirements can vary. In general, the provisions grant consumers the right to know what information companies are collecting and how it is being used while also requiring consent or providing the option to opt out of certain data uses.

While there are commonalities among the state laws, there are also differences in provisions. Odia Kagan, partner and chair of the EU General Data Protection Regulation compliance and international privacy at Fox Rothschild LLP, notes variations in areas such as the treatment of sensitive data, precise geolocation data, website disclaimers, and the regulation of targeted advertising.

The implementation dates for the new laws vary. The Iowa law will take effect on January 1, 2025, followed by Tennessee on July 1, 2025, and Indiana on January 1, 2026.

Some states have adopted unique approaches to privacy legislation. For example, the Florida measure primarily targets specific large tech companies while awaiting the approval of Governor Ron DeSantis. On the other hand, the Montana bill, awaiting action from Governor Greg Gianforte, offers more comprehensive protections, including the ability for consumers to use opt-out signals across multiple websites to express their privacy preferences.

The consumer advocacy group Consumer Reports has expressed the need for stronger privacy requirements in most states that have passed comprehensive privacy measures this year. The group has criticized certain aspects, such as the Florida law's limited applicability and the Tennessee law's weak enforcement mechanisms.

The impact of these new requirements on businesses will vary depending on the extent to which they already comply with existing privacy laws. For companies falling within the scope of a state privacy law for the first time, a substantial amount of work may be done. However, businesses that have already taken a proactive approach to privacy compliance by limiting data collection and conducting risk assessments will likely have a smoother transition. Odia Kagan suggests that for such companies, the new state laws may not significantly alter their existing compliance efforts.

Saunders adds that national companies are already recognizing the potential for additional state laws and are considering national rollouts of privacy measures rather than waiting for individual states to act. This proactive approach allows businesses to stay ahead of the evolving legal landscape and adapt their privacy practices accordingly.

As the number of states with comprehensive privacy laws continues to grow, businesses must stay informed about the evolving requirements and ensure their

practices align with the various state regulations. By proactively addressing consumer data privacy concerns, companies can maintain compliance, build trust with their customers, and mitigate potential legal risks.

<https://www.jdjournal.com/>