The Shifting Landscape of U.S. State Data Privacy Laws in 2024

The Legal Intelligencer

September 17, 2024

Coraleine Kitt

The landscape of U.S. state data privacy laws in the U.S. has grown increasingly complex in 2024. Seven additional states have enacted comprehensive privacy laws, raising the total number of states having their own privacy laws to nineteen. This figure could potentially increase to twenty with the inclusion of the controversial Florida Digital Bill of Rights. Aside from the number of new laws enacted in 2024, the considerable differences in the scope and content of these laws are of significance. This year marks a shift away from the previous dominance of the privacy law model set by Washington State Privacy Act (WPA), indicating a change in the states' approaches to privacy protection.

Key Trends in Data Privacy Legislation

While the WPA has influenced many state privacy laws enacted between 2021 and 2023, 2024 saw a growing divergence in legislative approaches, making it clear that the era of widespread adherence to the WPA model is coming to an end. Notably, Maryland passed a law that introduces unique data minimization provisions, while states like Vermont and Maine also proposed more restrictive measures, though they ultimately failed to pass.

This shift reflects a growing recognition among lawmakers that existing privacy laws may not adequately protect consumers, particularly in the face of rapidly advancing technology and evolving business practices. States are experimenting with new approaches that challenge industry norms, such as Maryland's heightened restrictions on sensitive data collection. These variations are creating a patchwork of laws that businesses will need to navigate carefully, raising the stakes for compliance efforts.

Maryland's Groundbreaking Approach to Data Minimization

One of the most significant developments in 2024 was Maryland's enactment of the Maryland Online Data Privacy Act (MODPA). After years of attempts to pass privacy legislation, Maryland's new law is widely regarded as the most consumer-friendly privacy law in the country. Its approach to data minimization, in particular, represents a substantial departure from the WPA model and may set the tone for future state privacy laws.

MODPA requires controllers to limit their collection of personal data to what is reasonably necessary to provide a product or service requested by the consumer. For sensitive data, the law imposes even stricter requirements, allowing collection only if it is "strictly necessary" to provide the service. This provision contrasts sharply with the WPA and other states' laws, which typically require consumer consent for sensitive data processing or, in some cases, merely an opt-out option. Maryland's law also prohibits the sale of sensitive data entirely, positioning the state as a leader in consumer privacy protections.

This shift towards more aggressive data minimization requirements has sparked debate. On one hand, privacy advocates argue that such measures are essential to curbing excessive data collection. On the other hand, critics contend that the practical implications of these provisions remain unclear, particularly regarding the definition of a product or service and the role of consumer consent. These questions may need to be resolved through future litigation or regulatory guidance.

The Legislative Landscape in Vermont and Maine

In Vermont and Maine, lawmakers also pursued comprehensive data privacy laws with a focus on data minimization, though both bills ultimately failed to pass. Vermont's proposed law, which included a limited private right of action for consumers to sue companies over sensitive data processing, was vetoed by the state's governor after an intense lobbying campaign by business interests. Maine's bill, which similarly sought to impose stricter data collection limits, stalled in the state Senate.

These legislative battles highlight a broader debate over the role of state privacy laws in regulating data collection practices. While proponents of stricter laws argue that current regulations do not go far enough in protecting consumer privacy, opponents maintain that overly restrictive rules could stifle innovation and create compliance challenges for businesses. Despite these setbacks, the push for stronger data privacy protections in these states is unlikely to disappear. Vermont's lead sponsor has already pledged to reintroduce the bill in 2025, suggesting that the fight for more robust privacy laws will continue.

The Recasting of the Connecticut Data Privacy Act

The evolution of the state privacy law debate is perhaps best exemplified by the changing perception of the Connecticut Data Privacy Act (CDPA). When the law was enacted in 2022, it was hailed as one of the most consumer-friendly privacy laws in the country, comparable to Colorado's law. However, in just two years, the CDPA has been recast by some privacy advocates as an insufficient safeguard against invasive data collection practices.

During the Maryland legislative hearings, for instance, the CDPA was criticized as an industry-friendly law that failed to meaningfully curb harmful practices. This shift in perception underscores how quickly the privacy law landscape is evolving and how concepts that were once widely accepted can be challenged as new voices and perspectives enter the debate.

New Models and Updates in State Privacy Laws: Minnesota, New Jersey, and Rhode Island

While some states are pushing the boundaries of privacy law, others continue to build upon existing models. Minnesota's Consumer Data Privacy Act (MCDPA), passed in 2024, closely follows the WPA framework but includes novel provisions such as the right to challenge adverse profiling decisions and specific rules for handling precise geolocation data. The law also requires controllers to maintain a data inventory, a requirement that could become more common as states refine their privacy laws.

New Jersey's law similarly builds on the WPA model, though it broadens the definition of sensitive data to include financial information. It also mandates rulemaking, making it only the third state, after California and Colorado, to do so. Rhode Island's law, on the other hand, diverges from the WPA by including unique privacy notice requirements and omitting the common data minimization provisions found in other state laws.

These variations indicate that while the WPA model remains influential, states are increasingly adapting privacy laws to address specific local concerns and emerging issues, such as the handling of geolocation data and financial information. For businesses, this means that compliance will become more complex as states introduce laws with varying requirements.

Similar Privacy Laws: Kentucky, Nebraska, and New Hampshire

Not all states are advancing novel privacy frameworks. In 2024, Kentucky, Nebraska, and New Hampshire enacted privacy laws that closely mirror existing statutes from other states. Kentucky's law, for instance, follows the model of Virginia's privacy law, while Nebraska's legislation is based on Texas' statute. New Hampshire drew from an earlier version of Connecticut's privacy law before it was amended in 2023.

For businesses operating across multiple states, these similar laws offer a degree of consistency, but they also highlight the importance of thoroughly understanding the nuances between various state laws. As more states pass privacy legislation, even minor differences in wording or scope can create significant challenges for ensuring full compliance.

Amending Existing Privacy Statutes

In addition to new laws, several states have amended their existing privacy statutes in 2024. California led the way with six amendments to the California Consumer Privacy Act (CCPA), including new provisions for children's data, neural data, and updates to thresholds for the law's applicability. Colorado also passed three amendments, including new rules for biometric data and children's privacy, while Virginia and New Hampshire made more targeted updates.

These amendments reflect a broader trend of states revisiting their privacy laws to address emerging concerns and incorporate new technological developments. For businesses, this means that staying compliant requires not only understanding new laws but also keeping up with changes to existing ones.

The Challenge of Enforcement

While the number of states with comprehensive privacy laws continues to grow, enforcement of these laws remains in its early stages. Many states are still in the "right to cure" period, meaning enforcement actions are limited. However, California has already taken action against companies like DoorDash and Tilting Point Media for alleged violations of its privacy law.

Other states, such as Connecticut and Colorado, have also ramped up their enforcement efforts, with a focus on children's data and biometric information. As more states begin enforcing their privacy laws, businesses should expect increased scrutiny and the possibility of more public enforcement actions in the coming years.

Looking Ahead: The Future of State Privacy Laws

As state privacy laws continue to evolve, businesses will need to adapt to a complex and fragmented regulatory environment. While some states are pushing for stronger data minimization requirements and broader consumer rights, others are content to follow existing models. The trend of amending and updating privacy laws is also likely to continue, as lawmakers respond to new technological developments and privacy concerns.

For companies, this means that compliance efforts must be flexible and proactive. Staying ahead of changes in state privacy laws will be crucial to avoiding potential legal challenges and maintaining consumer trust. With federal privacy legislation stalled, the state-led approach to privacy regulation is here to stay, and businesses must be prepared to navigate this increasingly complex landscape.

ATTORNEYS MENTIONED

Coraleine Kitt, CIPP/US, CIPP/E