Convergence Among Comprehensive State Privacy Laws Points to Practical Data Risk Management Strategies

Summary:

- While there are multiple comprehensive state privacy laws with varying features, there are also significant areas of convergence.
- Those areas of convergence—such as risk assessments, notice and consent, and privacy rights—point to data mapping and governance as key data risk management priorities.

Comprehensive data privacy laws demand good governance and data risk management strategies. That demand will only increase in urgency with the rapid adoption of generative AI technologies. As of this writing and since 2018, 20 states have enacted such laws.[1] They are "comprehensive" because they govern how private-sector entities collect, process, and share personal information. While their enactment has lagged behind the explosion of data collection by businesses, their passage has also coincided with the current generative AI boom that we are living through. States have also been filling in the void created by congressional failure to pass a comprehensive federal privacy law, despite numerous attempts.

Comprehensive privacy laws have material consequences for organizations that fall within their scope, adding resource costs and creating compliance and litigation risks, often across multiple jurisdictions. Importantly, those risks run with the residence of the individual whose records are being processed, not with an organization's place of business. So even if your business is based in Massachusetts (which at the moment is considering, but does not have, a comprehensive privacy law), you may have obligations under the privacy laws of Connecticut, Virginia, Colorado, and Maryland (for example) if you collect personal information from residents of those states.

Predictably, this jurisdictional fragmentation can create confusion and frustration for organizations that must create policies, procedures, and frameworks to comply with diverse legal requirements. Fragmentation also encourages taking shortcuts, which creates dangers that might not be readily evident: for example, simply asking an AI chatbot to create a privacy policy, or finding a pre-existing template on the web or from a competitor, buys far more risk than it solves, since policies that do not match an organization's actual practices will invite consumer protection liability or allegations of misrepresentation.

But hiding behind points of divergence among state laws is a surprising amount of substantive convergence, suggesting that organizations concerned about mitigating their compliance and litigation risk can focus on key governance and risk management principles that will satisfy many of their compliance obligations.

The common denominator underneath it all is data mapping: the exercise of understanding the details of your organization's data flows. It is a key, and often poorly understood and undervalued, component of the privacy law landscape. But the time is now to begin the process.

Below is a list of three materially important, practical requirements that cut across data privacy laws and point to how organizations can understand what data they have, build their overall data strategy, protect personal information, and simultaneously do much of the work of complying with numerous state laws:

1. Risk Assessments.

18 of the 20 comprehensive data privacy laws currently enacted mandate some form of risk assessment (Utah and Iowa do not). Typically, the requirement to undertake a risk assessment is triggered when an organization processes certain kinds of identified sensitive information. For example, under recently-enacted regulations passed pursuant to the California Consumer Privacy Act (CCPA), businesses

must conduct risk assessments before processing consumer personal information that "presents significant risk to consumers' privacy." Such processing activities might include "selling or sharing" personal information, processing personal information defined as "sensitive" (such as government identifiers, precise geolocation, information concerning sexual orientation, racial or ethnic origin, religious or philosophical beliefs, union membership, and citizenship and immigration status). Under Connecticut's Data Privacy Act, a "controller" (that is, the entity directing the data processing activity) must conduct a data protection assessment for each processing activity that "presents a heightened risk of harm to a consumer." This includes among other things processing activities involving the sale of consumer data, processing sensitive data, or processing data for purposes of profiling if certain conditions are met. Maryland's Online Data Privacy Act has a substantially similar provision. And in Massachusetts, the version of the Massachusetts Data Privacy Act that passed the Senate in September 2025 (but is still being considered by the House, as of this writing) contains a strong version of this requirement.

The point of starting with risk assessments is that they demand governance, and determining whether a risk assessment applies to your organization's processing activities requires, first, understanding at a fundamental level your organization's data map. What information do you collect? Why do you collect it? What do you do with it? How long do you keep it? Who gets access to it? Who do you share it with, and why? Do you get compensated for sharing it? The risk assessment provisions of the vast majority of these comprehensive privacy laws cry out for understanding, at a granular level of detail, your organization's data processing systems and procedures. Doing so requires having individuals responsible for developing and appropriately documenting that understanding and then working from that posture of understanding to develop a comprehensive data strategy.

2. Notice and Consent.

Each comprehensive privacy law requires that notice be provided to individuals either prior to or at the point of data collection, in some way that is visible to the individual. In instances where sensitive data is being collected, consent might be required.

These provisions typically do more than simply require broad provisions in a privacy policy ("We might collect all of your data."). They often require that organizations provide details about categories of data being collected, whether the information is being shared, and what the purpose is for collecting the information. The Texas Data Privacy and Security Act, for example, requires that a controller provide a "reasonably accessible and clear privacy notice" that includes (a) the categories of data being processed, (b) the purposes for processing the data, (c) how consumers may exercise their rights, and (d) what categories of data are shared with third parties. The New Jersey Data Protection Act has similar provisions. So does the Utah Consumer Privacy Act, often considered a business-friendly privacy law.

Compliance with this provision will flow down from the work an organization must do to understand its data map. Just like knowing whether an organization is processing information that may present risks to consumers requires understanding what data is being processed, so does being able to provide a guide to individuals about what they can expect is going to be done with their personal information at the point of collection.

3. Data Subject Rights.

Every state provides for some set of privacy rights that individuals have for organizations that fall within the scope of the law. Organizations are sometimes caught flat-footed when they receive some kind of data subject access request (DSAR), passing the request along to counsel for purposes of compliance. But responding to such a request—whether it is to delete information, opt out of the sale of information, or simply to know what is being processed about an individual—requires that the entity have done the work of mapping data: it should already know what data it collects and where that data lives to a reasonable level of confidence. Data subject rights further require organizations to be able to have mechanisms to (a) intake DSARs, (b) respond to them timely, and (c) locate and evaluate the data they have.

Being able to respond to DSARs appropriately, or craft notices and consents, or undertake risk assessments, requires resource-intensive, up-front work. That work involves standing up and maintaining (and continually improving) organizational governance, including policy controls and identification of individuals within the organization who are responsible for responding to requests, assessing the accuracy of notices, and determining the organization's data processing risk posture. These responsibilities are made more complex by the increasingly complex picture painted by generative AI technologies, which organizations are adopting at a rapid clip and which an increasing number of businesses are using to process vast amounts of organizational data. Rapid AI adoption and evolution of AI tech recommend taking these governance steps now: they are good practice, will allow for easier integration of more complex data processing over time, and have the added benefit of putting organizations in greater compliance with comprehensive data privacy laws. These points of convergence reveal that mapping—and the governance it requires—is an essential key to an organization's data processing risk management strategy.

[1] CA, CO, CT, DE, FL, IA, IN, KY, MD, MN, MT, NE, NH, NJ, OR, RI, TN, TX, VA, UT.