JENNER&BLOCK

"A Look at 5 States' News Data Privacy Laws," *Law360*

Publications

October 7, 2024
By: Madeleine Findley, David C. Layden

In their article for *Law360*, Partners Michelle Kallen, Madeleine Findley, and David Layden and Associate Daniel Echeverri discuss the impact of data privacy laws that have recently taken effect in five states and how companies can understand what the laws regulate and enforce.

Former Associate Peggy Xu and former SEO Law Fellow Daniel Freedline contributed to this article.

State data privacy laws are increasingly relevant to the ways companies collect, process and disseminate data.

In the last few years, nearly 20 states have passed comprehensive data privacy laws, with several already in effect. The regulation and enforcement of data privacy at the state level creates significant challenges and risks for enterprises that operate businesses, interact with employees and consumers, and provide and use technologies in multiple jurisdictions.

Utah, Florida, Texas, Oregon and Montana have data privacy laws that have taken effect or are coming into force this year. Three of these laws — the Florida Digital Bill of Rights, the Texas Data Privacy and Security Act, and the **Oregon Consumer Privacy Act** — went into effect at the beginning of July.

The Utah Consumer Privacy Act became effective Dec. 31, 2023, and the Montana Consumer Data Privacy Act became effective Oct. 1. To address compliance in a timely manner and to avoid unwittingly generating risks, it is important that companies understand what these five statutes regulate and how they will be enforced.

Laws' Similarities and Differences

The data privacy laws in Utah, Florida, Texas, Oregon and Montana share certain similarities. All five states grant consumers rights over their personal data, including the right to access, correct — with the exception of Utah — and delete personal data in the possession of a data controller, and to opt out of targeted advertising.

All five states also include carveouts for information governed by the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act, the Family Educational Rights and Privacy Act, and the Driver's Privacy Protection Act — although Utah does not exempt institutions subject to HIPAA and Oregon only exempts institutions subject to its state banking law.

Additionally, none of the five state laws applies to data about consumers acting in a commercial or employment context.

But the similarities largely stop there. The state privacy laws diverge, for example, in their applicability criteria. The data privacy statutes in Florida, Montana, Oregon and Utah set thresholds to determine which entities are subject to enforcement. Entities that control or process the personal data of a minimum specified number of consumers or those who derive a specified percentage of gross revenue from the sale of personal data are covered by the law.

Of the five states, the Texas Data Privacy and Security Act's applicability criteria is the most expansive, applying broadly to any person conducting business in Texas who produces products or services targeted to Texas residents and who processes or sells personal data, with an exception for "small businesses" as defined by the U.S. Small Business Administration. Montana's law also has a similar exception.

Meanwhile, Florida's Digital Bill of Rights has the narrowest threshold, applying only to controllers with over $1 billion in global revenue and that: derive 50% of gross annual revenue from online advertisement sales; operate a smart speaker device; or operate an app store offering at least 250,000 applications.

Compared to data privacy statutes in the other states, Florida's law is unambiguously targeted at Big Tech companies, though it does contain provisions — particularly those governing children's interaction with websites and online services — that apply more broadly.

The state privacy laws also differ in their definitions of "personal" and "sensitive" data.

In all five states, "sensitive data" refers to a subset of personal data that either (1) reveals an individual's ethnic or racial origin, religious beliefs, mental or physical health condition, sexual orientation, citizenship or immigration status, or geolocation data; or (2) involves the processing of genetic or biometric personal data to identify a specific individual.

But some states include unique protections for certain categories of data.

Oregon, for instance, defines "sensitive data" to include data revealing a consumer's "status as transgender or non-binary" and "status as a victim of a crime," while Montana, like California, includes data revealing "information about a person's sex life," wording that is far more expansive than the "sexuality" or "sexual orientation" language adopted by most other states.

Moreover, the Florida and Texas laws require businesses to post disclaimers, including on their websites, regarding certain data sales using required language: "NOTICE: we may sell your [sensitive or biometric] personal data."

The data privacy laws in the five states compared in this review also vary substantially in their enforcement provisions. Although state attorneys general are solely entrusted with enforcement of the data privacy statutes in all five states, their enforcement authority varies significantly. In Utah, for example, the attorney general may pursue enforcement actions only upon referral from the Utah Division of Consumer Protection.

Moreover, although each state's data privacy statute includes a right to cure, which gives alleged violators the opportunity to remediate before facing enforcement actions, cure periods vary in length between states. Notably, in Florida a cure period is not guaranteed and is subject to attorney general discretion,[1] and alleged violations involving a known child are barred from receiving any opportunity to cure whatsoever. Moreover, the cure periods in Oregon and Montana sunset in January and April 2026, respectively, while they do not expire in Utah or Texas.

The remedies and maximum penalties available to state attorneys general also differ by state. In Utah, only civil penalties are available, and they are capped at $7,500 per violation plus actual damages. Although Texas and Oregon share the same $7,500 cap for civil penalties, their state attorneys general may also seek injunctive relief and reasonable fee recovery.

Meanwhile, Florida and Montana confer the most power on their respective attorneys general. In enforcing violations of the Florida Digital Bill of Rights, Florida's attorney general may seek declaratory judgment, injunctive relief and civil penalties of up to $50,000 per violation plus actual damages, with this number trebled if the violation involves a known child. The Montana Consumer Data Privacy Act is even more expansive, as it does not specify — and therefore does not limit — the relief the state attorney general may seek, nor does it stipulate a maximum civil penalty.

Regulatory Risks

The data privacy laws in the five states we analyzed have only gone into effect within the last few months — and in Montana's case, will not take effect until later this year. As such, the exact enforcement risks presented by each statute remain to be seen. Nonetheless, the textual differences in each statute illustrate the regulatory challenges businesses may face in each of the

five states.

Texas's data privacy law, for example, is the most broadly applicable of the states we analyzed. Except for small businesses as defined by the U.S. Small Business Administration, all entities conducting business in Texas that process or sell personal data are subject to regulation under the Texas Data Privacy and Security Act. In addition, the Texas attorney general has assembled a team "focused on aggressive enforcement of Texas privacy laws"[2] and taken actions against data brokers and car manufacturers, underscoring that consumer privacy is a high enforcement priority for the state.

This, combined with Texas's large population and market size, implicates a higher level of regulatory risk for companies compared to the other four privacy statutes analyzed above.

Oregon is also notable due to its expansive definitions of personal data and sensitive data, which also increase regulatory risk for companies covered by the law. Despite these broad definitions, Oregon does allow alleged violators to recover reasonable fees if they can demonstrate that there was no reasonable basis for the enforcement action, but this is untested and may prove to be a difficult standard to meet.

Florida's Digital Bill of Rights poses unique regulatory risks compared to the other four states. Although many aspects of Florida's privacy statute are more narrowly targeted at Big Tech, its enforcement provisions are among the most stringent.

Moreover, the Florida Digital Bill of Rights contains several substantive provisions about children's online privacy — unlike the other four states, Florida's privacy statute also regulates how online platforms process the personal and geolocation data of minors, as well as how businesses acquire information from minors online. These regulations apply to online platforms providing services, products, games and/or features "likely to be predominantly accessed by children," and so extend much more broadly than the provisions aimed at large tech companies.

The Montana Consumer Data Privacy Act's applicability criteria are the second-most expansive of the five states, meaning more businesses could be subject to regulation compared to the other states. Montana's empowerment of its attorney general also goes farther than the four other states we analyze, with the sole limitation on the attorneys general enforcement authority — a 60-day cure period — expiring in 2026.

Montana's smaller population size and market presence, however, may ultimately limit the risk this statute presents.

Of the five states, Utah appears to pose the least amount of regulatory risk. The Utah Consumer

Privacy Act, which has been in effect the longest of the five, creates the fewest consumer rights and has some of the narrowest applicability criteria of the privacy laws we analyze above.

As such, fewer businesses fall under the Utah statute, and those who do enjoy a more permissive regulatory environment compared to the other four states. Moreover, data controllers in Utah enjoy a 30-day cure period and the Utah attorney general cannot seek declaratory relief, injunctive relief or fee recovery.

Action Steps

These five state data privacy laws are still nascent — only time will tell how different state attorneys general put their enforcement provisions to use. Businesses should keep apprised of these and other data privacy laws, including the developments around the proposed federal American Privacy Rights Act. For now, businesses should:

- Determine whether they are subject to the new and upcoming state data privacy laws;
- Update their privacy policies to ensure compliance with any applicable state data privacy laws;
- Review their consumer-facing data request processes to account for the growing number of states empowering residents with additional rights; and
- Proactively monitor and assess their internal data practices to avoid any potential exposure to enforcement by the state attorneys general, particularly in Texas, Oregon and Florida.

Related Attorneys

Madeleine Findley
Partner
mfindley@jenner.com
+1 202 639 6095

David C. Layden
Partner
dlayden@jenner.com
+1 312 923 2796

Related Capabilities

Data Privacy and Cybersecurity

Related Locations

Chicago

Washington, DC

Stay Informed →