Stay Current

PAUL HASTINGS

June 2026

Follow us on LinkedIn

PH Privacy

New State Privacy Rules Require Businesses to Assess High-Risk Activities and Regulate Disclosures of Sensitive Data

By Aaron Charfoos, Michelle Reed, Jeremy Berkowitz

Businesses will need to take a closer look at upgrading their privacy programs as states consider more stringent laws on the collection and processing of personal data. In 2026, four states — Oklahoma, Louisiana, Alabama and Vermont — have passed comprehensive new state privacy laws. Additionally, three states — Virginia, Maryland and Connecticut — have passed significant amendments to their privacy laws, some of which are expected to go into effect next month.

This flurry of legislation is largely similar to past state frameworks, although there seems to be greater emphasis on data protection impact assessment requirements, protections around the sale of data, and disclosures on the use of automated decision-making and large language models.

With a federal privacy law still unlikely, businesses will need to determine whether and how they need to comply with these requirements and take further steps to operationalize their privacy programs.

New Comprehensive State Privacy Laws

Four states this year have passed new comprehensive statewide privacy laws: the Oklahoma Consumer Data Privacy Act, the Louisiana Data Privacy Act, the Alabama Personal Data Protection Act and the Vermont Data Privacy and Online Surveillance Act. The Oklahoma and Louisiana laws both go into effect on Jan. 1, 2027, the Alabama law goes into effect on May 1, 2027, and the Vermont law goes into effect on Jan. 1, 2028. All four laws have largely similar frameworks in terms of applicability thresholds and requirements, but some take unique nuances on certain privacy matters.

Applicability/Thresholds

All four laws apply to businesses that conduct business in the state or target each state's residents with products and services. Here are the threshold requirements for each law:

- Oklahoma:
  - Control or process the personal data of at least 100,000 consumers; or
  - Control or process the personal data of at least 25,000 consumers and derive more than 50% of gross revenue from the sale of personal data.

- Louisiana:
  - Have annual gross revenue greater than $25 million;
  - Annually buy, receive, sell or share for commercial purposes the personal data of 75,000 or more consumers or households; or
  - Derive 50% or more of annual revenue from selling or sharing consumers' personal data.
- Alabama:
  - Control or process the personal data of more than 25,000 consumers (excluding data processed solely for payment transactions); or
  - Derive more than 25% of gross revenue from the "sale" of personal data.
- Vermont:
  - Control or process the personal data of at least 35,000 consumers;
  - Control or process the sensitive data of at least 3,000 consumers; or
  - Offer for sale the personal data of at least 3,000 consumers.

All four states also provide entity-level exemptions for businesses that already must comply with the Gramm Leach Bliley Act and Health Insurance Portability and Accountability Act, as well as for higher-education institutions and nonprofits. Additionally, none of the laws apply to data collected in an employment context or B2B data. The Alabama law provides an additional exemption for businesses with fewer than 500 employees.

Notice Requirements

All four laws require covered businesses to have privacy notices that are transparent and easy to understand. Notice requirements are generally similar to what is in other state privacy laws, including providing information on the categories of personal data collected, the purposes of processing personal data and consumers' data subject rights as it relates to the personal data. Additionally, Vermont requires information on whether the business collects, uses or sells personal data for the purpose of training large language models.

Data Protection Impact Assessments

The Oklahoma, Louisiana and Vermont laws all require that businesses conduct data protection impact assessments for high-risk activities, including but not limited to targeted advertising, sale of personal data and profiling. These assessments must consider the benefits of the processing against the potential risks to consumers, taking into account available safeguards, including de-identification, consumer expectations and the nature of the business relationship with consumers.

Vermont specifically requires a separate assessment for businesses that engage in profiling for decisions producing legal or similarly significant effects (e.g., hiring, firing, lending decisions), with prescribed components including purpose disclosure, risk analysis, categories of data used, performance metrics, transparency measures and post-deployment monitoring.

Here are a few other points of distinction:

- **Effective Date**: The attorneys general in Oklahoma, Louisiana and Vermont will have the right to request and review the data protection impact assessments. The assessment requirement goes into effect for both Oklahoma and Louisiana on Jan. 1, 2027, while the requirement for Vermont goes into effect on Jan. 1, 2028.
- **Alternative Assessments**: Both Oklahoma and Louisiana allow businesses to use similar data protection impact assessments completed for other states.
- **Retroactivity**: Oklahoma, Louisiana and Vermont require assessments for all ongoing activities and new activities that start after Jan. 1, 2027, not activity completed prior to this date.

Data Subject Rights

All four state laws provide the following rights:

- Right to access personal data and confirm whether a controller is processing it
- Right to correct inaccuracies
- Right to delete personal data
- Right to data portability
- Right to opt out of targeted advertising, the sale of personal data, and profiling that produces legal or similarly significant effects

It should be noted that Alabama requires explicit consent for targeted advertising or sales of personal data for children ages 13–15. For children under the age of 13, businesses are required to follow the Children's Online Privacy Protection Act to process personal data.

Enforcement

For all four laws, the states' attorneys general are responsible for enforcement and there is no private right of action. All four states allow a cure period:

- Louisiana: Seven months
- Alabama: 45 days
- Oklahoma: 30 days
- Vermont: 60 days, but it is currently only in effect until June 30, 2029

Amended Privacy Laws

Virginia Consumer Data Protection Act (VCDPA) Amendment: Geolocation Data Ban (SB 338)

This amendment goes into effect on July 1, 2026. Virginia's existing VCDPA permitted the sale of "precise" geolocation data — information capable of determining a person's location within a 1,750-foot radius — if consumers affirmatively consented (opt-in). SB 338 replaces that consent-based framework with a categorical ban: No business may sell or offer for sale precise geolocation data, regardless of consumer consent. The law applies regardless of consumer opt-in consent, eliminating any prior consent

defense. Data brokers and advertising technology companies must immediately review and cease any sale of precise Virginia consumer geolocation data by July 1.

Maryland Data Privacy Act (HB 711)

This amendment goes into effect on July 1, 2026 and expands Maryland's definition of sensitive data to include data inferred by a controller based on personal data that, alone or in combination with other data, is used to indicate any category of sensitive attributes. This "inferred sensitive data" provision is notably broader than most existing state privacy frameworks.

The amendment prohibits businesses from knowingly selling personal data of a consumer if the controller knew or should have known that the purchaser intends to use that data for immigration enforcement by a governmental unit that has engaged in or supported civil immigration enforcement within the previous six months. Public records custodians must also:

- Adopt rules and procedures to prevent unauthorized disclosure of personal information.
- Deny access requests for public records for immigration enforcement purposes absent a valid judicial warrant.

Connecticut SB-1295; SB-4

There are two amendments to Connecticut's Data Privacy Act. The first, SB-1295, signed into law in June 2025, goes into effect on July 1, 2026, and includes the following provisions:

- **Applicability**: The Connecticut law now applies to entities that (1) process personal data of at least 35,000 consumers (down from 100,000), (2) process any consumers' sensitive data or (3) offer consumers' personal data for sale — with no volume threshold for the last two triggers.
- **Sensitive Data**: The definition of sensitive data now covers Social Security numbers and drivers' licenses, and the sale of sensitive data is now banned without individual consent.
- **Notices**: Privacy notices must now disclose whether the entity uses or sells personal data to train large language models.
- **New Consumer Rights**: Connecticut residents can now request a list of third parties to whom their personal data was sold, access to inferences derived from their data and additional information about how their data is used, similar to obligations in the Rhode Island Data Transparency and Privacy Protection Act.
- **Profiling Impact Assessments**: Companies that engage in profiling to make decisions with legal or significant effects must perform a new "impact assessment" covering the personal data involved and the profiling's purpose, risks, mitigation measures and post-deployment monitoring. This applies to all new processing activities created after Aug. 1, 2026.

On May 27, 2026, SB-4 was signed into law as an additional amendment. Most of these requirements take effect on Oct. 1, 2026, while the data broker registration requirements take effect on Jan. 1, 2027. This bill includes the following key changes:

- **Geolocation Data**: Businesses are now prohibited from selling consumers' "precise geolocation data," defined as information derived from technology including GPS coordinates or other mechanisms that directly identify the specific location of an individual within a radius of 1,750 feet.

- **Surveillance Pricing**: Businesses must make disclosures regarding their use of surveillance pricing.

- **Facial Recognition Technology**: Businesses that use facial recognition technology for fraud prevention purposes must provide notice at the time such technology is being used, as well as a link to the company's policy around it.

- **Data Broker Requirements**: Connecticut now requires all data brokers doing business in the state to register with the Department of Consumer Protection by Jan. 1, 2027. The law also requires the commissioner of consumer protection to establish an accessible deletion mechanism by July 1, 2028, allowing consumers to submit a single deletion request to all registered data brokers. Data brokers must comply with deletion requests submitted through this mechanism once every 45 days, beginning Oct. 1, 2028. Data brokers will also be subject to independent third-party audit requirements once every three years, beginning in 2031.

Next Steps

Given the accelerating pace of state privacy legislation, businesses should consider the following:

- Assess how these laws apply to your operations based on geography, consumer data volumes and revenue composition.

- Conduct or update your records of processing/data mapping exercises to inventory what consumer data you collect, where it is stored and how it is shared.

- Review and update privacy notices, website disclosures and consumer request handling procedures.

- Audit vendor and processor contracts to ensure required data protection provisions are in place, including those that prohibit sale of precise geolocation data or other sensitive data.

- For businesses covered by the Connecticut and Virginia laws, immediately review geolocation data licensing and advertising technology contracts. All sales of precise consumer geolocation data must cease by July 1, 2026, for Virginia and Oct. 1, 2026, for Connecticut.

- Establish or update data protection impact assessment procedures for high-risk processing activities covered under the Oklahoma, Louisiana, and Vermont laws.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Aaron Charfoos
+1-312-499-6016
aaroncharfoos@paulhastings.com

Michelle A. Reed
+1-972-936-7475
michellereed@paulhastings.com

Jeremy Berkowitz
+1-202-551-1230
jeremyberkowitz@paulhastings.com