SQUIRE PATTON BOGGS

Adding to the Count

The latest in state consumer privacy laws

August 2026

2026 started with 20 state consumer privacy laws (SCPLs), three of which went into force on January 1, 2026. During the first half of 2026, four new SCPLs were added, bringing the count to 24 – all since the California legislature passed the California Consumer Privacy Act (CCPA) in June 2018.

Also, during the first half of 2026, state legislatures enacted significant amendments to their existing SCPLs. We cover the state privacy laws developments in this first of a three-part series on mid-year US data law updates – stay tuned for updates on teen online privacy and safety, as well as AI.

Other than new double opt-in consent requirements in the Vermont and Louisiana SCPLs for certain data sales, the four new SCPLs do not add new "high watermark" requirements for most organizations but do have some noteworthy nuances. The trend among amendments enacted during the first half of 2026 is to add more restrictive requirements – particularly with respect to sensitive personal data (especially for minors and precise geolocation data), prohibitions on certain personal data sales and limits on profiling activities. The amendments do create new high watermark requirements, thereby making the SCPL patchwork more difficult to navigate, especially for an organization that intends to avoid certain high-water marks to prevent material negative business impact.

At the same time, Senator Ron Wyden (D-OR) sent a letter to attorneys general in 11 states with SCPLs that require universal opt-out signals (like Global Privacy Control). The letter asked the attorneys general to set the expectation (via guidance) that an organization will honor preference/opt-out signals received from their states' residents, regardless of the residents' actual physical locations or IP addresses. Senator Wyden's letter states that geolocation filtering based on IP addresses is a "flawed" method of determining residency (e.g., a user may be temporarily out-of-state), thereby allowing organizations to "selectively ignore consumer opt-out requests." Whether geofiltering based on IP address will remain an acceptable method for determining state residency is unclear. But, given the increasingly restrictive requirements related to personal data sales and sharing, adopting a national high-water approach to opt-out signals may become operationally necessary, even when some types of marketing and analytics are negatively impacted.

The new laws enacted in 2026

The four new SCPLs enacted this year are:

1. Alabama Personal Data Protection Act – Effective May 1, 2027
2. Louisiana Data Privacy Act – Effective January 1, 2027
3. Oklahoma Act Relating to Data Privacy – Effective January 1, 2027
4. Vermont Data Privacy and Online Surveillance Act – Effective January 1, 2027

All four apply only to personal data of state residents who are acting in the personal, family or household context, and not in the business-to-business or employment contexts.

In the Vermont SCPL, personal data explicitly includes "derived data," which is "created by the derivation of information, data, assumptions, correlations, inferences, predictions or conclusions from facts, evidence, or another source of information or data about a consumer's device." (§ 2415a(19)) This definition is similar to guidance under the CCPA that inferences about a person created by an organization are personal information.

Like the majority of the SCPLs, the new SCPLs exclude "de-identified data" and "publicly available data" from the definition of personal data.

The definitions of de-identified data in the four new SCPLs require that the controller (i) takes reasonable measures to ensure that the de-identified data cannot be associated with an individual; (ii) publicly commits to maintain and use the data only in a de-identified form and to not attempt to reidentify the de-identified data and (iii) contractually obligates any recipient of de-identified data to comply with (i) and (ii).

The Vermont SCPL's cites the de-identification requirements in the HIPAA Privacy Rule as a "reasonable" measure to prevent reidentification (9 V.S.A. § 2415a18(A)(ii)). (The Iowa and Nebraska SCPLs do not include the same three requirements.)

The Alabama SCPL adds a use-based requirement for de-identified data, i.e., a controller "in possession of" de-identified data must take measures to ensure that the de-identified data cannot reasonably be associated with an individual; must refrain from reidentifying the de-identified data when maintaining and using de-identified data and must contractually obligate recipients of the de-identified data to comply with these requirements. (The Florida SCPL also adds an additional requirement, i.e., a controller must implement business processes to prevent the inadvertent release of de-identified data.)

What organizations are in scope?

The four new SCPLs all have entity-level and data-level exemptions familiar from the SCPLs already in force. Two notable nuances relate to the monetary and processing thresholds:

- The monetary and processing thresholds in the Alabama SCPL are not linked to a specific timeframe. Compare this to the processing thresholds in the other new SCPLs, which are measured by annual revenue or annual amounts of personal data purchases, sales or sharing (Louisiana), or by "a calendar year" (Oklahoma).
- The Vermont SCPL thresholds are measured based on the preceding calendar year, i.e., the entity either:
  - Controlled or processed the personal data of not fewer than 35,000 consumers during the preceding calendar year
  - Controlled or processed the sensitive data of not fewer than 3,000 consumers during the preceding calendar year
  - Offered for sale in trade or commerce the personal data of not fewer than 3,000 consumers during the preceding calendar year

The Vermont SCPL's thresholds do not apply to "consumer health data" (CHD), which is "personal data that a controller uses to identify a consumer's physical or mental health condition, diagnosis or status, including gender-affirming health data and reproductive or sexual health data." Instead, the CHD-related restrictions (§ 2415k) apply to a "a person that conducts business in [Vermont] or a person that produces products or services that are targeted to residents of [Vermont]" (§ 2415b(b).) (The Connecticut and Maryland SCPLs also define and regulate CHD.)

Sensitive personal data processing

The definition of sensitive data in the four new SCPLs follows the general trend, as do the four new SCPLs' requirements to obtain consent prior to the collection and other processing of sensitive data (subject to customary exceptions).

For children's data, the new SCPLs require that a controller process personal data of a "known child" (under age 13) in compliance with the Children's Online Privacy Protection Rule (COPPA). Only the Louisiana SCPL defines "known child," i.e., "when a controller has actual knowledge of, or willfully disregards, the child's age" (i.e., the COPPA standard).

The Vermont SCPL's inclusion of the following as sensitive data results in a broad definition: CHD (defined above) and "a consumer's financial account number, financial account login information or credit card or debit card number that, in combination with any required access or security code, password or credential, would allow access to a consumer's financial account."

The Alabama and Vermont SCPLs require consent for processing of personal data for targeted advertising for personal data sales when a controller (i) has actual knowledge that a consumer is age 13 to 15 (Alabama – like the Montana and New Hampshire SCPLs) or (ii) has actual knowledge and willfully disregards that the consumer is age 13 to 17 (Vermont – like the Connecticut and Maryland SCPLs).

The Vermont SCPL also prohibits processing for purposes of targeted advertising and personal data sales when a consumer is age 13 to 17 (§ 2415e(7)), and also requires compliance with the Vermont Age Appropriate Design Code Act (VAADC) for "covered businesses," i.e., conducting business in Vermont and generating most revenue by offering online services that are reasonably likely to be accessed by a minor (under age 18). The VAADC requirements include privacy by default settings and design feature restrictions. If the VAADC and the Vermont SCPL conflict, then the "provisions of the law that afford the greatest protection for the right of privacy for consumers shall control."

Separate laws in Alabama (in force January 1, 2027) and Louisiana (in force July 1, 2027) require app store providers and app developers to implement age verification, parental consent, data minimization and other requirements for minor users. (More on these laws and the VAADC in the third installment of our midyear update.)

The Vermont SCPL's CHD provisions also prohibit use of "a geofence to establish a virtual boundary that is within 1,850 feet of any health care facility, including any mental health facility or reproductive or sexual health facility, for the purpose of identifying, tracking, collecting data from or sending any notification to a consumer regarding the consumer's consumer health data," as well as the additional consent discussed below. The Connecticut SCPL also includes a geofence restriction for consumer health data (§42-526) as do laws in Nevada (NV Rev Stat §603A.540), New York (NY Gen Bus L § 394-G), and Washington (RCW §19.373.080),

Other obligations regarding sensitive personal data sales in the Louisiana and Vermont SCPLs are discussed below.

Personal data sales

The Oklahoma SCPL defines "sale" as the exchange of personal data for monetary consideration (the minority definition), whereas the other three new SCPLs include "other valuable consideration" (the majority definition). Alabama's definition of sale adds "and the third-party is not restricted in its subsequent uses of the personal data," and two uncommon exclusions: the disclosure or transfer of personal data to a third-party for the purpose of providing analytics services or marketing services solely to the controller, which is not in any other SCPL. These uses could be structured as transfers to a processor (or s service provider in the CCPA) under other SCPLs, which transfers are excluded from "sale."

One of the most notable differences among the new SCPLs is an additional consent (i.e., in addition to the general sensitive data processing consent) for sensitive data sales. The Louisiana SCPL requires that a person or entity that derives 50 percent or more of its annual revenues from selling consumers' personal information "may not engage in the sale of personal data that is sensitive data without receiving prior consent from the consumer." (R.S. 51: §1780.4.P.(1).) The Vermont SCPL also requires an additional consent for CHD: "A person shall not [...] "sell, or offer to sell, consumer health data without first obtaining the consumer's consent." (§ 2415k(4).)

The Louisiana SCPL also requires an enhanced presale notice (similar to the Texas and Florida SCPLs) for sensitive data: "For sales of sensitive data, the following notice in the same manner as the privacy notice is required: "NOTICE: We may sell your sensitive personal data." If the sensitive data is biometric data, a second notice is required, i.e., "NOTICE: We may sell your biometric personal data."

Consumer rights

All four of the new SCPLs offer the familiar consumer rights to confirm, correct, delete, obtain a copy and opt out of targeted advertising, sale and profiling in furtherance of a decision that produces a legal or similarly significant effect concerning a consumer.

Of the four new SCPLs, only the Vermont SCPL offers a consumer right to right to obtain a list of the third parties to which a controller has sold the consumer's personal data (If the controller does not maintain the information in a format specific to the consumer, a list of third parties to whom the controller has sold any consumers' personal data may be provided instead). Compare the third-party list right in the Vermont SCPL to the right in the Connecticut SCPL, which applies to the specific third parties to which the controller sold personal data, and the Minnesota SCPL, which requires a list of specific third parties to which the controller disclosed personal data. All four of the new SCPLs include a requirement, which is common in SCPLs, that the privacy policy disclose the categories of personal data sold to third parties (or "shared" in the Oklahoma SCPL) and categories of the recipient third parties. (See also the "Privacy Notice" section below.)

A consumer's right to obtain a copy of the consumer's personal data is limited to data "in a digital format" under the Louisiana and Oklahoma SCPLs. The latter also limits the right to personal data processed by automated means.

The Alabama SCPL's right to confirm explicitly includes data processed by a processor or third-party acting on a controller's behalf. For the right to delete, the controller must delete "the consumer's personal data," a potentially broader definition. The other three new SCPLs require a controller to delete personal data that was provided by or obtained about the consumer.

The Vermont SCPL has the broadest right to confirm; it includes any inference about the consumer derived from the consumer's personal data, and the ability to confirm whether a controller or processor is processing the consumer's data for profiling purposes in furtherance of a decision that produces a legal or similarly significant effect.

The term "profiling" is defined as any form of "solely automated" processing in the Alabama, Louisiana and Oklahoma SCPLs. The right to opt-out of profiling in the Alabama SCPL is limited to solely automated decisions but is not so limited in the other new SCPLs.

The Vermont SCPL has the broadest rights related to profiling. First, profiling is more broadly defined as "any form" of automated processing. Second, a Vermont consumer has the right to opt out of profiling for an automated decision and the right to question the result of the profiling. If the profiling concerns housing, the consumer also has the right to correct any incorrect personal data and have the profiling decision reevaluated based on the correct data. (The SCPLS of Connecticut and Minnesota also have broader profiling related rights, but the Minnesota SCPL does not limit the right to correct housing related decisions.)

The Alabama and Vermont SCPLs both require one or more secure and reliable methods for a consumer to exercise rights, whereas the Louisiana and Oklahoma SCPLs require two or more methods.

Only the new Alabama SCPL does not offer appeal rights, and only the Oklahoma SCPL does not include provisions related to authorized agents. The Alabama SCPL allows authorized agents but does not have explicit provisions on the designation process. The Louisiana and Vermont SCPLs, however, provide the right to designate an authorized agent using a technology, including a link to a website, an internet browser setting or extension or a global setting on an electronic device, that allows for opt out of processing for targeted advertising, for sale of personal data, or for both.

Opt-out

All four new SCPLs offer consumers the right to opt-out of sale, as well as for processing for targeted advertising. The Louisiana and Oklahoma SCPLs condition the controller's obligation to process opt-out requests on authentication, but do not require authentication. Authentication of consumer opt-out requests is optional in the Alabama and Vermont SCPLs, but the two laws only permit a controller to reject an opt-out request if the controller has a reasonable suspicion of fraud, or for the Alabama SCPL a reasonable suspicion that the requestor is not authorized to make the request.

The Alabama, Louisiana and Vermont SCPLs require a controller to provide consumers with an opt-out preference signal (OOPS) (also known as universal opt-out mechanism), such as the Global Privacy Control or other link to a website that enables a consumer to directly opt-out (Alabama), a link to a website, an internet browser setting or extension, or a global setting on an electronic device that allows the consumer to indicate the consumer's intent to opt-out (Louisiana); or a platform, technology or other mechanism (Vermont). Using the OOPS must allow a consumer to opt-out of the processing of personal data for the purpose of targeted advertising, for personal data sales or both. If the link is not provided, under the Alabama SCPL, a controller must then provide up-to-date contact information for a consumer to submit an opt-out request.

Under the Alabama and Vermont SCPLs, if a consumer's decision to opt-out of any processing of the consumer's personal data for the purposes of targeted advertising, or for personal data sale through an OOPS conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty program, the controller must honor the consumer's OOPS, but may notify the consumer of the conflict and allow the consumer to confirm the controller-specific privacy setting or participation in the loyalty program. This approach differs somewhat, in material ways, from other SCPLs (especially the California and Colorado SCPLs), making a single national approach to the resolution of OOPS related conflicts difficult if not impossible.

Privacy notice

The general privacy notice requirements in the new SCPLS follow the majority approach of not requiring the kind of specific formatting and substance required in the California and Colorado SCPLs. They also do not have separate "notice at collection" obligations like the CCPA.

The new SCPLs in Alabama and Oklahoma require that a privacy notice list the categories of third parties with which personal data is shared, and the categories of personal data shared with those third parties – similar to the Delaware and Maryland SCPLs. Of the SCPLs, only the CCPA defines "share," which means disclosures for cross-context behavioral advertising. Despite the use of the undefined term "share", all of the SCPLs exclude processors from the definition of third parties, as long as the required privacy contracting terms are in place.

The Louisiana and Vermont SCPLs require that a privacy notice lists the categories of third parties to which personal data is sold, and the categories of personal data sold to those third parties. Compare these requirements to the Minnesota SCPL, which requires that the privacy notice list the categories of third parties to which personal data is sold or shared, the Oregon SCPL which requires that the privacy notice describe all categories of third parties that the controller shares (but not sells) personal data and the Connecticut SCPL, which requires that the privacy notice disclose the third parties to which personal data is sold (but not shared).) The term "sale" excludes a transfer to an affiliate except in the CCPA and Florida SCPL.

The Rhode Island SCPL is the notable outlier, requiring that the privacy notice "identify all third parties to which the controller has sold or may sell "personally identifiable information" (§ 6-48.1-3(a)).

If a controller makes any retroactive material change to its privacy notice or practices, the Vermont SCPL requires that the controller "provide a reasonable opportunity for consumers to withdraw consent to any further and materially different collection, processing or transfer of previously collected personal data" following the material change. (The SCPLS of Connecticut, Montana and Minnesota are similar).

The Vermont SCPL requires that a privacy notice includes a statement disclosing whether the controller collects, uses or sells personal data for the purpose of training large language models. Only the Connecticut SCPL has a similar requirement. Neither of these laws define "training" or "large language models."

Data processing agreements

All four new SCPLs follow a similar structure for contracting requirements between a controller and a processor consistent with the majority approach. Of the four new SCPLS, only the Vermont SCPL requires a processor to provide a controller with the opportunity to object to a subcontractor. (The SCPLs of Colorado and Connecticut each have a similar opportunity to object requirement.) No new contract term obligations are necessitated by the new SCPLs, which means existing contracting high watermarks are sufficient.

Risk assessments

The Alabama SCPL does not require that a controller conduct a data processing risk or impact assessment. Both the Louisiana and Oklahoma SCPLs require risk assessments for high-risk processing activities as of January 1, 2027, and are not retroactive. The Vermont SCPL begins one year later for high-risk processing activities created on or generated after January 1, 2028. The definition of high-risk processing follows the majority approach. None of the new SCPLs include detailed substantive requirements for assessments. Assessments are subject to regulatory inspection, but no filing or attestation requirements like those in the CCPA apply.

Cure period

The four new SCPLs do not provide for private rights of action and offer cure periods after a notice of noncompliance from the relevant state regulator. The cure periods are:

- **Alabama**: 45 days with no expiration
- **Louisiana**: 30 days until July 31, 2027
- **Oklahoma**: 30 days
- **Vermont**: 60 days until June 30, 2029

Amendments enacted in 2026

Amendments enacted in 2026 follow the same general trend as amendments enacted in 2025: stricter requirements for controllers.

Key amendments enacted in 2025 and now in force are:

- **Connecticut**: Profiling and sensitive data
- **Kentucky**: Data protection impact assessment requirements for profiling that presents a foreseeable risk of an unlawful disparate impact on consumers
- **Oregon**: Prohibitions on sales and targeted advertising with known minors' data or precise geolocation data

The Connecticut SCPL's amendment enacted on May 27, 2026 is in force on October 1, 2026; it adds a definition, and establishes new requirements, for facial recognition technology; amends the definition of publicly available information (by adding new exclusions); and prohibits controllers and third parties from selling any consumer's precise geolocation data. The Connecticut SCPL's 2026 amendment also extends the consumer right to delete to "publicly available information that is (i) collated and combined to create a consumer profile that is made available to a user of a publicly accessible Internet web site for compensation or free of charge, or (ii) made available for sale, or [...] any inference generated from" the foregoing."

The Maryland SCPL's 2025 amendment is in force as of July 1, 2026. This amendment modifies the 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 data, and also restricts the sale of personal data to governmental entities that, within the last six months, engaged in or supported immigration enforcement. None of the other SCPLs include a similarly specific requirement.

The New Hampshire SCPL's 2026 amendment is in force on January 1, 2027, and prohibits a controller from selling personal data of child (i.e., under age 13).

The New Jersey SCPL's 2025 amendment is in force as of January 20, 2026, and exempts certain personal data and entities from certain requirements concerning notification and disclosure of personal data regarding the federal Health Insurance Portability and Accountability Act (HIPAA), protected health information (as defined in the HIPAA), insurance organizations and national securities associations.

Most of the New Jersey SCPL's June 2026 amendment went into effect immediately and prohibits a controller from selling sensitive data, without any minimum threshold before the prohibition applies. The June 2026 amendment's provisions establishing a public registry of data brokers and data collectors enter into force 270 days after June 30, 2026. The New Jersey attorney general announced that enforcement of the data broker law is delayed until after the public registry system is launched. Some in New Jersey's political establishment have expressed concern that the loss of access to demographic data about voters (e.g., race, national origin and religion) from data brokers will negatively impact their fund raising and campaign activities and are urging reconsideration.

The Virginia SCPL's 2026 amendment is in force as of July 1, 2026, and prohibits the sale or offer for sale of precise geolocation data concerning a consumer. (A 2025 amendment is preliminarily enjoined.)

On June 16, 2026, the Delaware legislature also passed House Bill 380, an amendment that significantly lowers the processing thresholds, adds new requirements for privacy impact assessments, data minimization and consumer rights (among other changes). As of the date of this blog post, House Bill 380 still shows as "ready for Governor for action".

Takeaways

One of the most notable aspects of the SCPL amendments is the trend toward banning or restricting sensitive personal data sales and precise geolocation data in particular:

- **Maryland and New Jersey**: All sensitive personal data sales banned
- **Connecticut and Virginia**: Sale of precise geolocation data banned
- **Oregon**: Processing for targeted advertising or profiling of known minors' personal data (under age 16) and sale of precise geolocation data banned
- **Connecticut SCPL**: Sale of personal data for minors (under age 18) banned
- **New Hampshire SCPL**: Sale of personal data of children under age 13 banned

The new SCPLs in Vermont and Louisiana pick up this trend: Vermont requires an additional consent for the sale of CHD and Louisiana requires an additional consent to sale of sensitive personal data, as well as an enhanced notice.

The California legislature is considering similar legislation: AB 322 would ban precise location sales and AB 1542 would prohibit sale or sharing of any sensitive personal information. Information rights regarding third-party disclosures (discussed above), and requirements related to personal data of children/teens/minors (which we will cover in the third of this midyear series) also require heightened obligations, but the SCPLs lack uniformity in their approaches.

Most organizations update their privacy notices and compliance programs in the second half of the year. (The CCPA requires annual updates.) The 2026 updates offer a good opportunity to apply the requirements of the four new SCPLs and the amendments, as well as to conduct an overall compliance gap assessment and address gaps. This process also can help an organization prepare for the potential of a California compliance audit, which CalPrivacy has recommended as its compliance efforts have expanded. Other issues to be addressed before year end are the CCPA's risk assessments and preparation for cybersecurity audits. (When conducted under direction of outside counsel, the process and work product has the potential for attorney–client privilege protection.)

To help organizations manage the similarities and differences among the SCPLs, we developed comparison charts broken down by key topics, which are available on an annual subscription basis (including quarterly updates). More information is available here or contact the authors.

The authors would like to thank paralegal Krista Setera for her invaluable assistance.

Contacts



Julia Jacobson
Partner, New York
T +1 212 872 9832
julia.jacobson@squirepb.com



Alan Friel
Partner, Los Angeles | Atlanta
T +1 213 689 6518
alan.friel@squirepb.com

The opinions expressed in this update are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

© Squire Patton Boggs. All Rights Reserved 2026.

71932/08/26