SQUIRE PATTON BOGGS

The Second Half of the Year Brings New State Privacy Obligations

Are You Ready?

US – July 2025

Many businesses have worked diligently to comply with the 13 state consumer privacy laws ("CPLs") in effect in the first half of 2025 (14 CPLs if Florida is included). Some businesses have chosen to comply on a state-by-state basis and others have followed the high-watermark approach of applying the strictest standard from among the CPLs to all states with CPLs or on a nationwide basis. Regardless of the chosen approach, in the second half of 2025 brings a new batch of CPLs, some with material differences from the earlier CPLs. In addition, amendments to CPLs already in effect will bring new obligations and requirements for many businesses during the second half of 2025. Accordingly, if these changes were not prospectively addressed, now is the time to confirm which of the new CPLs and amendments are applicable, and timely revise privacy notices and compliance program procedures. Also, with the increase in CPL enforcement, and the growing size and frequency of civil penalties, now also is a good time for an overall privacy compliance checkup.

A list of the 20 CPLs and their effective dates and applicability thresholds is included in this appendix.

The New CPLs

During the second half of 2025, three CPLs come into effect ("Q3-Q4 CPLs") and another three are effective as of January 1, 2026 ("2026 CLPs"):

- Tennessee Information Protection Act
  effective July 1, 2025
- Minnesota Consumer Data Privacy Act
  effective July 31, 2025
- Maryland Online Data Privacy Act
  effective October 1, 2025
- Kentucky Consumer Data Protection Act
  effective January 1, 2026
- Rhode Island Data Transparency and Privacy Protection Act
  effective January 1, 2026
- Indiana Consumer Data Protection Act
  effective January 1, 2026

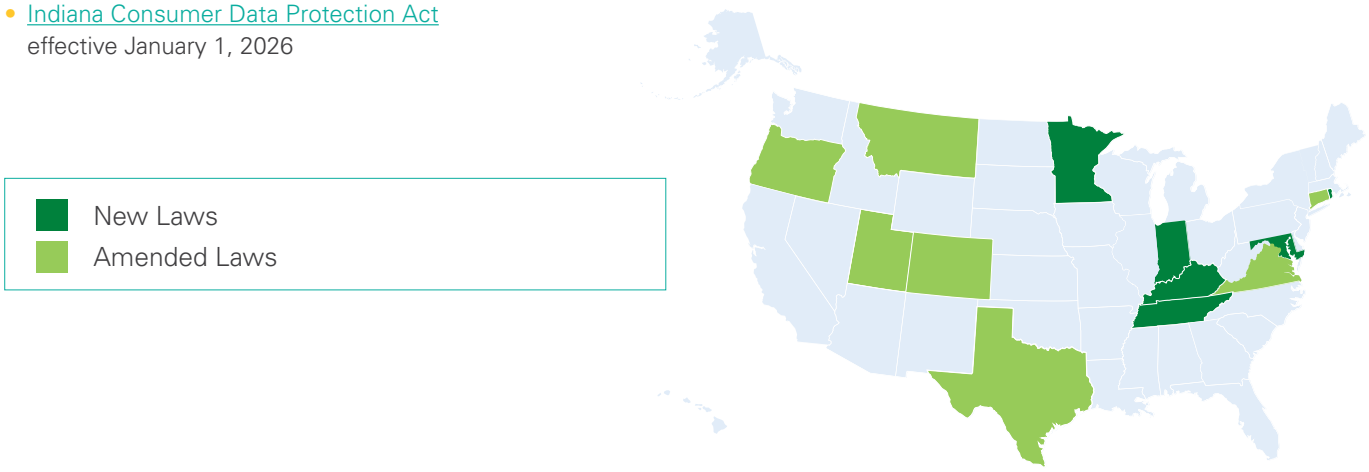
The Amended CPLs

Three of the CPLs already in effect have significant amendments effective during the second half of 2025: Colorado, Montana and Oregon. Six more amendments are effective during 2026: Connecticut, Indiana, Kentucky, Oregon, Utah and Virginia.

Also New

An amendment to the Texas Data Broker Law, effective September 1, 2025, expands the definition of, and thresholds of coverage for, data brokers and also increases transparency obligations. In addition, two states enacted new minor-focused privacy laws (Arkansas and New York), and two states enacted age-appropriate design laws (Nebraska and Vermont), joining the enjoined California Age-Appropriate Design Code Act and the Maryland Age-Appropriate Design Code Act. Watch – or, better yet, subscribe to – Privacy World for an upcoming blog post about these minor-focused laws issues.

If a business has not already built the new and amended CPLs into prior updates to its privacy notice and compliance program, then, assuming the applicability thresholds are met and no exemptions apply, addressing the Q3-Q4 CPLs and 2026 CPLs, as well as CPL amendments effective between now and January 1, 2026, can help create efficiencies by mitigating the need to make multiple rolling updates. This also can reset the notice 12-month lookback in the California Consumer Privacy Act (CCPA), thereby helping avoid a year-end rush to address the new and amended 2026 CLPs and CCPA lookback. A business may, however, wish to reserve the right to honor new or changed consumer privacy rights only as and when the rights are in effect.



Key Compliance Considerations

Consumer Privacy Rights and Privacy Notice Requirements

While the new CPLs include consumer privacy rights similar to current CPLs, they also include noteworthy deviations. One key area of deviation relates to the information rights of consumers about third-party recipients of personal data sales and certain other disclosures.

The Minnesota CPL requires that a controller provide a consumer with the right to obtain a list of specific "third parties" to which the controller has disclosed personal data. (Note that processors and their affiliates are not third parties.) If the controller does not maintain the list in a format specific to the consumer making the request, then the controller may provide a list of specific third parties to whom the controller has disclosed any consumer's personal data. This is a significant burden but should be a familiar obligation to controllers subject to the Oregon CPL.

We recommend that controllers subject to the Minnesota CPL and the Oregon CPL view this requirement as applicable to disclosures to "third parties," which includes "sales," resulting from third-party cookies. Like the majority of the CPLs, the Minnesota CPL and Oregon CPL define "sale" as an exchange of personal data for any valuable consideration. (Only Indiana, Iowa, Kentucky, Tennessee, Utah, and Virginia define "sale" as an exchange for monetary consideration only.) Also, this disclosure obligation is retrospective, not a snapshot in time, but is subject to exemptions.

The Maryland CPL – like the Delaware CPL – requires a list of categories of third-party recipients as to the specific consumer or, if the controller does not maintain the recipient categories list in a format specific to the consumer, a list of the categories of recipients of any consumer's personal data will suffice. Requiring categories of recipients, rather than specific recipients, is much less burdensome.

An amendment to the Montana CPL (effective October 1, 2025) requires that a controller's privacy notice include an "explanation" of consumer rights, in addition to the currently-effective requirement for a description of how consumers may exercise their consumer rights. This explanation requirement is consistent with other CPL requirements; i.e., privacy notices must clearly explain the privacy rights available to consumers and how consumers can exercise them. We have seen enforcement inquiries by state regulators taking issue with unclear explanations of which privacy rights apply to residents of which state.

However, the most significant new privacy notice requirements are in the Rhode Island CPL. Effective January 1, 2026, the Rhode Island CPL's first operative section applies to a "website or internet service online service provider" that is subject to Rhode Island jurisdiction ("Online Service"). This definition of Online Service provider is both broader (because no thresholds apply) and narrower (because it applies online only) than "controller."

An Online Service provider must, however, designate a controller if the provider collects, stores and sells "personally identifiable information" of "customers" (which is defined similarly to "consumers" in the other CPLs). The term "personally identifiable information" is not defined, (§ 6-48.1-4(a)), and whether this term is intended as narrower than "personal data," which is used in all other sections of the Rhode Island CPL, is unclear.

Like the majority of the CPLs, the Rhode Island CPL defines "sale" as an exchange of personal data for any valuable consideration. But, unlike the other CPLs, an Online Service provider must include in its privacy notice details about "all third parties" to which the controller "has sold or may sell" its customers' personally identifiable information. For some Online Service providers, the inclusion of "may sell" will require ongoing privacy notice updates, such as for sales to new third parties. As with the Oregon and Minnesota CPLs, complying retrospectively with the disclosure obligations is a challenge, especially as to cookies, which can frequently change. A "controller" also must clearly and conspicuously disclose sales of personal data for targeted advertising (§ 6-48.1-3(b)). No specific posting requirements apply in the subsection that requires this targeted advertising disclosure but, presumably, the "conspicuous location on its website or online service platform where similar notices are customarily posted" from the prior subsection (§ 6-48.1-4(a)) applies.

Also noteworthy: effective July 1, 2026, an amendment to the Connecticut CPL adds new disclosure requirements in § 42-520, such as a statement in the privacy notice disclosing "whether the controller collects, uses or sells personal data for the purpose of training large language models" (among other new requirements).

Profiling/ADM

Given Congress' failed attempt to impose a preemptive moratorium on state laws regulating artificial intelligence ("AI") and profiling and automated decision-making ("ADM") that use AI, the addition of new CPLs regulating profiling and ADM is especially notable.

Except for the CPLs of Iowa and Utah, the CPLs regulate profiling and/or ADM that uses personal data, but the details vary. Rulemaking under the (CCPA) detailing the rights and obligations apply to profiling and ADM remains ongoing, but the most recent version of the CCPA regulations lessens the impact on businesses. New Jersey regulators also are working on rulemaking, and Colorado regulators have promulgated complex regulations regarding profiling, including information and appeal rights, subject to exceptions.

The Maryland and Tennessee CPLs allow a consumer to opt out of profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer. The CPLs of Delaware, Maryland, Montana, New Hampshire and Rhode Island also include the "solely" modifier, as do the draft CCPA regulations. An amendment to the Montana CPL (effective October 1, 2025) removes the "solely" modifier. An amendment to the Connecticut CPL also removes the "solely" modifier (effective July 1, 2026). All other CPLs do not limit the opt-out right to profiling based on solely automated decisions.

The Minnesota CPL offers consumers the distinct rights: to question the result of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer; to be informed of the rationale behind each decision; and, if feasible, to be informed of what actions the consumer might have taken to secure a different decision and the actions that the consumer might take to secure a different decision in the future. A Minnesota consumer also has the right to review his or her personal data used in the profiling. If the decision is based upon inaccurate personal data (considering the nature of the personal data and the purposes of the processing of the personal data), the consumer has the right to correct the personal data and to have the profiling decision reevaluated based upon the corrected personal data (§ 325O.05(1)(g)). While the other Q3-Q4 CPLs and 2026 CPLs offer profiling opt-out rights, none of them include rights like those in the Minnesota CPL.

The obligations regarding use of personal data for profiling based on automated decisions, together with the draft CCPA regulations, have created a complex patchwork. Given the operational impact to businesses, especially those operating in the "not solely" states, a high-water mark approach may not function as well as in other areas of CPL compliance. (Our state CPL comparison charts discussed below include profiling and ADM requirements.)

Sensitive Personal Data, Sensitive Processing and Purpose Limitations

The Minnesota CPL prohibits personal data processing for targeted advertising and personal data sales without a consumer's consent when a controller knows that the consumer is between age 13 and age 16 (§ 325M.16(2)(f)).

The Maryland CPL's approach to sensitive data processing is stricter than other CPLs: a controller cannot collect, process or share sensitive data unless the collection or processing is strictly necessary to provide or maintain a specific product or service requested by the consumer, (§ 14-607(A)(1)), or sell sensitive personal data (§ 14-607(A)(2)). Even the Maryland CPL's purpose limitation for non-sensitive personal data is limited to what is "reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer" (§ 14–4607 (B)). Prior to the end of the legislative session, the Maryland House considered (but did not pass) an amendment that would have adjusted this limitation to "adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer." This change would have better aligned with other CPLs.

How Maryland's purpose limitations will impact digital advertising to adults is unclear, but sales of personal data and processing for the purposes of targeted advertising are prohibited if the controller knows or should have known that the consumer is under age 18 (§ 14-607(A)(4),(5)) – the highest age of any of the currently effective CPLs. The Maryland CPL also includes provisions specific to "consumer health data."

Effective January 1, 2026, an amendment to the Oregon CPL prohibits (i) sales of personal data when the controller has actual knowledge that, or willfully disregards whether, that consumer is under 16 years of age, and (ii) sales of data that accurately identify past or present precise geo-location (within a radius of 1,750 feet) that links or is linkable to a consumer, but excluding the "content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility" (§ 646A.578 (2)(d)). As noted above, the Maryland CPL prohibits sensitive data sales and precise geolocation data is a type of sensitive data.

An amendment to the Colorado CPL adds new requirements for processing of a minor's personal data when the processing presents "heightened risk of harm to minors," effective October 1, 2025. An amendment to the Virginia CPL related to minors and social media is effective January 1, 2026, and an amendment to the Connecticut CPL adds new requirements as to minors. (More on minors in an upcoming Privacy World post.)

As of July 1, 2025, obligations related to biometric data were added to the Colorado Privacy Act ("Biometric Data Amendment"). The monetary and processing thresholds that apply to the rest of the Colorado Privacy Act do not apply to a controller that processes biometric data under the Biometric Data Amendment. A controller is in scope "regardless of the amount of biometric identifiers or biometric data controlled or processed annually" (§ 6-1-1304(1)(b)).

If a controller does not meet the processing threshold with respect to other categories of personal data, then the controller must comply only with the Biometric Data Amendment. Employers also are in scope of the Biometric Data Amendment. Employers may require, "as a condition of employment," employees' or prospective employees' consent to collect and process biometric identifiers for certain enumerated purposes (§ 6-1-1314(6)(a)); processing biometric identifiers for other purposes requires consent, but the employer may not require consent "as a condition of employment or retaliate against an employee or prospective employee who does not consent to such collection or processing" (§ 6-1-1314(6)(b)).

The Biometric Data Amendment also adds some new written policy and privacy notice requirements for controllers, as well as the obligation to allow a broader right of access for biometric data than for other personal data. A processor of biometric data also has a new requirement for a protocol for responding to a data security incident that may compromise the security of the biometric data entrusted to the processor by the controller (§ 6-1-1314(3)). Neural data was added as a new sensitive data category, reflecting the special sensitivity of the data collected from increasing use of mental health apps and so-called "brain wearables" outside of traditional healthcare settings.

The amendment to the Connecticut CPL effective July 1, 2026, adds new sensitive data categories (including neural data and government issued IDs) (§ 42-515) and prohibits sales of sensitive data without consent (§ 42-520(a)(1)(H)).

Our CPL comparison charts also cover regulation of sensitive personal data, including processing purpose limitations.

Opt-Out Preference Signal (OOPS)

The CPLs of Maryland and Minnesota require a controller to make available an OOPS (also known as global privacy control or universal opt-out mechanism) for consumers to exercise their rights to opt out of use of their personal data for targeted advertising and to opt out of the sale of their personal data. In both laws, a consumer may designate an agent using an OOPS (Maryland, § 14-4606; Minnesota, § 325M.14(2)(d)).

Of the CPLs already in effect, the CPLs of California, Colorado, Connecticut, Delaware, Montana, Nebraska, New Hampshire, New Jersey, Oregon and Texas also have OOPS requirements. With twelve CPLs requiring them, many businesses are considering whether to honor OOPS nationally.

Risk Assessment and Other Information Governance

Documented risk assessments for processing deemed high risk are required in the Q3-Q4 CPLs (Tennessee, Minnesota and Maryland), as well as the 2026 CPLs (Kentucky, Rhode Island and Indiana). The draft CCPA Regulations include assessment requirements (read more), leaving the CPLs of Iowa and Utah as the only ones that do not, or do not plan to, require assessments. Many believe the lack of enforcement on assessment requirements already in effect, even with respect to businesses under investigation for other issues, relates to the still-ongoing CCPA rulemaking, which seems to be nearing completion.

The Minnesota CPL requires documentation of data inventories (§ 325M.16(2)(c)), as does the current draft of the CCPA regulations. The Minnesota CPL also requires a controller to document and maintain a description of the policies and procedures specific to compliance with the Minnesota CPL, including the name of the chief privacy officer or other individual with oversight responsibility.

The Tennessee CPL provides a limited affirmative defense for violations if the controller's privacy program "reasonably conforms" to the National Institute of Standards and Technology Privacy Framework or comparable privacy framework (§ 47-18-3213).

As noted above, the Biometric Data Amendment to the Colorado CPL added some new written policy requirements for biometric identifiers and biometric data that supplement the current "Documentation Concerning Duties of Controllers" in the Colorado Privacy Act Rule 6.11 and also new security incident response policy requirements for processors.

Contacts

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

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

Kyle Dull
Senior Associate, New York & Miami
T +1 212 872 9867
E kyle.dull@squirepb.com

See our **Appendix** that lists the 20 CPLs, their effective dates and applicability thresholds.