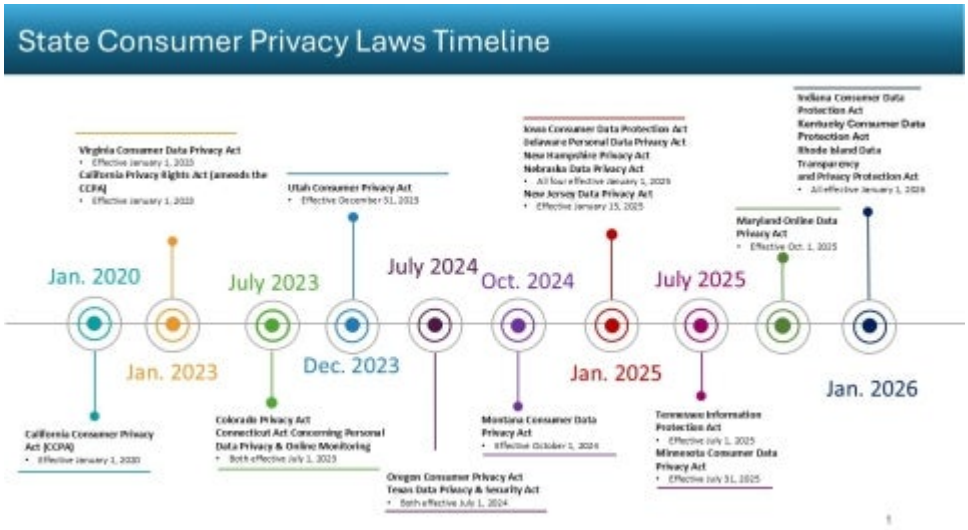
Updates
December 17, 2024
Privacy Law Recap 2024: State Consumer Privacy Laws

U.S. privacy law continued to expand in 2024, both geographically and substantively.

We now have 19 states with comprehensive consumer privacy laws (some of which are already in effect, while others become effective in 2025 and 2026). This recap focuses on the 10 state laws that were enacted or took effect this year—specifically in Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, and Texas—as well as the states that enacted meaningful updates.

Through this lens, we highlight the trends taking shape across the U.S. consumer privacy landscape and discuss important nuances among this year's 10 newly enacted or effective state laws. The emerging trends help establish a relative baseline for the contents of these laws and what we might expect from future legislation. Meanwhile, the nuances addressed below reflect how states continue to iterate on the existing frameworks in ways that could have significant compliance impacts.



U.S. State Privacy Laws by Effective Date

Emerging Trends in State Comprehensive Consumer Privacy Laws

Who These Laws Protect

In keeping with the current norms, all 10 of the comprehensive consumer privacy laws enacted or effective in 2024 protect the personal data of "consumers" within their states—residents of that state, excluding individuals acting in employment or commercial contexts. The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), remains the only comprehensive state privacy law that applies equally to consumers, employees, and business-to-business commercial contacts.

The 10 states also maintain the general status quo of having distinct roles and responsibilities for those who determine the purpose and means of processing (controllers) versus those who process personal data on behalf of controllers (processors).

Definition of Personal Data

Each of the 10 states define "personal data" as any information that is linked or reasonably linkable to an identified or identifiable natural person. Oregon's law explicitly includes data that is linked to a "device that identifies, is linked to, or is reasonably linkable to one or more consumers in a household" in its definition, although all of the states' definitions arguably cover this data given their breadth.

Like their predecessors, the 10 state laws directly or indirectly exempt "de-identified" data and "publicly available" information (though definitions vary). For data to be considered de-identified, most states require controllers to (1) take reasonable measures to ensure that the data cannot be associated with a natural person, (2) publicly commit to maintaining and using de-identified data without attempting to reidentify it, and (3) contractually obligate recipients to adhere to the same technical and notice obligations.

States take varying approaches to "pseudonymous data," generally defined as data that can no longer be attributed to a specific individual without the use of additional information, so long as such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data are not attributed to a specific individual. As a subset of personal data, pseudonymous data is not always subject to the same level of requirements as "standard" personal data. For example, many of the 19

state privacy laws expressly exempt pseudonymized data from various consumer rights obligations.

Definition of Sale

Most of the 10 state laws track the definition of "sale" that originated in the CCPA as an exchange of personal data for monetary or other valuable consideration. Kentucky's law, however, joins six other state laws in excluding the "other valuable consideration" phrasing.

User Rights

Similar to the models set by the General Data Protection Regulation (GDPR) and the CCPA, all 10 of the state privacy laws enacted or effective in 2024 provide consumers with a number of rights regarding their data, including:

- **Right to know/access.** Consumers have the right to know whether the controller is processing their personal data and a right to access their data. Minnesota, like the CCPA, expressly prohibits the disclosure of certain information (*e.g.*, Social Security number, financial account numbers, account passwords, and biometric data). Instead, companies should inform the consumer that they collect this information without providing it directly.
- **Right to correct.** Consumers have the right to correct inaccuracies in their personal data—usually within 45 days of making the request—taking into account the nature and purposes of processing.
- **Right to delete.** Most of the 10 state laws follow the more common model, in which consumers have the right to delete personal data provided by, *or obtained about*, the consumer. Oregon's law extends this right to data "derived" about a consumer.
- **Right to portability.** Consumers have the right to obtain a copy of their data, so long as it is maintained in a technically feasible format. Notably, California amended the CCPA this year to clarify that personal information can exist in various formats, including abstract digital formats (*e.g.*, "compressed or encrypted files, metadata, or artificial intelligence systems that are capable of outputting personal information"). Ambiguity remains regarding how to interpret this amendment, particularly concerning its applicability to artificial intelligence models.
- **Right to opt out.** Consumers have the right to opt out of the "sale" and processing of their personal information for purposes of "targeted advertising." Companies generally comply by providing a clear and conspicuous method for consumers to opt out of such processing activities (*e.g.*, an opt-out link on their website's homepage). Eight of the 10 new laws joined the fray of states that require businesses to honor opt-out preference signals, like GPC, as valid requests to opt out.
- **Right to nondiscrimination.** Consumers have the right not to be discriminated against (*e.g.*, denied goods) for exercising their rights. This does not prohibit controllers from offering voluntary incentive programs wherein companies may generally charge or provide varying levels of service, provided they meet certain requirements for such programs.
- **Rights related to automated decision-making or profiling.** Consumers have the right to opt out of the processing of personal data for the purpose of profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer. Minnesota's law imposes a more expansive right to question the results of such profiling, discussed in detail below.
- **Right to appeal.** Consumers generally have the right to appeal the denial of any of their rights; the 10 newly enacted or effective laws each include this right.

Other Common Requirements

The 10 state laws generally contain the following common requirements, reflecting consistency with their predecessors:

- Specific contractual provisions must be included in agreements with service providers. The provisions are largely the same as those required by preexisting laws.
- Businesses must conduct a data privacy impact assessment (DPIA) to perform certain processing activities (*e.g.*, targeted advertising, sales, profiling, and sensitive data processing). Covered processing activities and required contents of DPIAs are generally consistent across state privacy laws.
- Privacy policies must contain certain information, with relatively few nuances among the contents required across the state laws.
- Businesses must establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data.
- Seven more states join California, Colorado, and Connecticut in expressly prohibiting the use of "dark patterns" to obtain user consent for any agreement, aligning with the Federal Trade Commission's prohibition of "dark patterns."

Enforcement and Cure Periods

Following the majority of states, violations under each of the 10 state laws are solely enforceable by the state attorney general, and they do not provide a private right of action. Apart from Maryland and Rhode Island, the other state laws include a mandatory cure period that varies depending on the state.

Nuances Among the 2024 Comprehensive Consumer Privacy Laws

Applicability Thresholds

Most state privacy laws include two tiers of applicability thresholds; the first is a default numerical value representing the number of in-state residents whose personal data are processed, and the other is a lower value that is tied to a revenue requirement from selling personal data. Texas and Nebraska eschew this standard of using numerical thresholds, instead regulating all persons that conduct business within their borders, process or sell personal data, and do not qualify as a small business as defined by the U.S. Small Business Administration.

New Consumer Rights

Some of the state laws introduce new or expanded consumer privacy rights. Oregon became the first state to require controllers to provide a list of specific third parties to which the controller disclosed either the specific requesting consumer's data or any personal data. Minnesota, Maryland, and Delaware contemplate similar rights, although some provide a narrower right to request a list of the *categories* of third parties that have received personal data from the controller.

As noted above, Minnesota introduces an extensive new right to question the results of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer. Consumers also have the right to (1) be informed of the reason that the profiling resulted in the decision; (2) if feasible, be informed of the 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; and (3) review the consumer's personal data used in the profiling. If the decision is determined to have been based upon inaccurate personal data, the consumer has the right to have the data corrected and the profiling decision reevaluated based upon the corrected data.

Definitions of Sensitive Data

Some of the state laws expand what constitutes sensitive personal information (SPI), including:

- **Biometric data.** Oregon and Maryland broaden the definition of "biometric data" by including information that, respectively, "allows or confirms" or "can be used" for unique identification of a person (rather than limiting the term to information that is or is intended to be used to identify a person).
- **Neural/biological data.** California and Colorado amended their definitions of sensitive personal data to include new data types—"neural data" in California and "biological data" in Colorado (which includes "neural data" as a subset). Colorado defines "biological data" as data generated by the technological processing, measurement, or analysis of an individual's biological, genetic, biochemical, physiological, or neural properties, compositions, or activities or of an individual's body or bodily functions that is used or intended to be used for identification purposes, either singly or in combination with other personal data. Both states define neural data similarly as information generated by measuring the activity of a consumer's central or peripheral nervous system and (in California) that is not inferred from nonneural information or (in Colorado) that can be processed by or with the assistance of a device.
- **Precise geolocation data.** All 10 state privacy laws generally treat precise geolocation data as SPI, and most define it as information collected from a technology or device that directly identifies the specific location of an individual within approximately one city block or a radius of 1,750 feet. Minnesota uniquely defines it by reference to decimal points of latitude/longitude coordinates.
- **Financial information.** New Jersey's law joins California's as an outlier that defines SPI to include financial information. Specifically, New Jersey defines SPI to include personal data revealing "financial information," which includes an account number, account log-in, financial account, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a consumer's financial account.

Restrictions on Processing Sensitive Data

Maryland takes a unique approach to regulating SPI by prohibiting companies from collecting, processing, or sharing a consumer's SPI unless strictly necessary to provide or maintain a specific product or service requested by that consumer. This contrasts with other states' SPI processing standards, most of which permit collecting and processing SPI based on the consumers' opt-in consent. Maryland also prohibits the sale of SPI, without exception.

Heightened Protections for Minors

Some of the state laws change the requirements for engaging in sales and targeted advertising concerning minors. Currently, companies must obtain consent prior to selling personal information, or engaging in targeted advertising, when the consumer is under the age of **16**. New Jersey and Delaware raise the bar by requiring opt-in consent for these activities when companies know the consumer is under the age of **17** (in New Jersey) or **18** (in Delaware). Maryland goes even further, replacing the consent requirement with a blanket prohibition of sales and ad targeting when a company knows or should have known that the consumer is under the age of **18**.

New Prohibitions and Operational Requirements

Some of the new laws introduce meaningful internal data governance requirements. Minnesota introduces the requirement to maintain an inventory of the data that must be managed as part of protecting the confidentiality,

integrity, and accessibility of personal data. Data inventories, or records of processing, are required under international data protection regimes, like the GDPR, but this is the first time we are seeing such a requirement expressly provided under the state privacy laws.

Maryland's law will also introduce some significant changes. For example, it imposes stringent data minimization obligations and permits the collection of personal information only in connection with products or services specifically requested by a consumer. This standard contrasts with other states' minimization standards, which permit collecting and processing personal information to the extent adequate, relevant, and reasonably necessary for the purposes disclosed to consumers at the time of collection.

Conclusion

In many ways, the state consumer privacy laws newly enacted or first effective in 2024 expand the scope of privacy requirements beyond those in the prior state laws and GDPR, so it is imperative that businesses understand their compliance obligations under this increasingly nuanced patchwork of privacy laws across the country.

This post is part of a series recapping privacy law developments in 2024. Please see the following Updates for further information:

- Privacy Law Recap 2024: Data Security
- Privacy Law Recap 2024: Regulatory Enforcement

Authors

Explore more in

Privacy & Security | Technology Transactions & Privacy Law | Litigation | Retail & Consumer Products | Digital Media & Entertainment, Gaming & Sports

Related insights

Update

Two Tools for Trump To Dismantle Biden-Era Rules: the Regulatory Freeze and the Congressional Review Act

Update

The FY 2025 National Defense Authorization Act: What's New for Defense Contractors