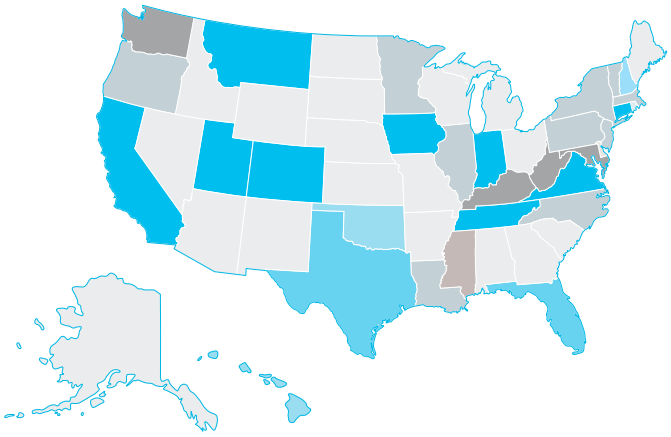
Clarip Readiness:
Complete 2023 US Privacy Law Tracker

State legislatures across the country continue to enact consumer data privacy laws, giving residents in their respective states more choice over how companies acquire and utilize their personally identifiable information (PII). One of the biggest issues companies are facing is the nuances of each states' regulations, thresholds, exemptions, cure periods or lack thereof, and time frames for responding to requests.



As of the 2022-23 legislative cycle, there are 11 states - California, Virginia, Colorado, Connecticut, Utah, Texas, Montana, Iowa, Tennessee, Indiana, and Oregon - that have enacted comprehensive data privacy laws. These 11 states represent 34% of the US population (over 100 million consumers).

During the 2022-23 legislative cycle, at least 16 states introduced privacy bills. Next year's legislative cycle has the potential to double the number of states with comprehensive privacy laws and will cover over half the US consumer population.

This seemingly patchwork approach to data privacy legislation can pose a compliance nightmare, and it increases liability risks for companies that operate in multiple states. In this document, we look at the laws that are currently in effect, enforcement dates, thresholds for covered businesses, definitions, exemptions, cure periods and potential fines for failure to comply, and time frames that companies have for responding to requests.

We take a look at:

(Click law to jump to page)

clarip

California's CCPA to CPRA

On January 1, 2020, the California Consumer Privacy Act of 2018 (CCPA) came into effect. Representing the United States' landmark comprehensive data privacy act, the CCPA is arguably the most comprehensive and the benchmark for all state level privacy laws. It imposes substantial privacy obligations on companies worldwide. The CCPA provides its residents with enhanced privacy rights. The California Attorney General began enforcing the CCPA on July 1, 2020. By November 2020, however, California voters approved the California Privacy Rights Act (CPRA), which significantly amended the CCPA.

The CPRA, effective July 1, 2023, amended and amplified the CCPA – many referred to it colloquially as "CCPA 2.0". As of July 1, the CPRA was meant to simply go away and become the new and improved CCPA. However, In a last-minute decision on June 30, 2023, the Sacramento County Superior Court ruled to push the effective enforcement of the CPRA amended regulations from July 1, 2023, to March 29, 2024.

The delay to March 2024 strictly pertains to data processing agreements, consumer opt-out mechanisms (Do not sell my information or my privacy choices in the footer of your website), mandatory recognition of opt-out preference signals (Global Privacy Controls), eliminating dark patterns, and consumer request handling.

Threshold changes for covered businesses

The CCPA/CPRA applies to for-profit institutions that "do business in California," collect and process personal information about California residents, and meet one of three thresholds:

(1) had **$25M in annual gross revenues** as of January 1 in the preceding calendar year, or

(2) buy, sell, or share the personal information of **100,000 California consumers or households**, or

(3) derives **50% or more** of its revenues from selling or sharing consumers' personal information.

In light of this revised text, most companies that triggered the coverage threshold based on annual revenues likely will continue to be covered, but many businesses that were covered by the CCPA merely because they collected the personal information of 50,000 devices (a threshold not difficult to trip for many online businesses), for example, will now fall outside the scope of the CPRA.

clarip

New Definitions

"Sensitive personal information" is defined as personal information that reveals:

- A consumer's social security, driver's license, state identification card, or passport number.
- A consumer's account log-in, financial account, debit card or credit card number combined with any required security or access code, password or credentials allowing access to an account.
- A consumer's precise geolocation.
- A consumer's racial or ethnic origin, religious or philosophical beliefs or union membership.
- The contents of a consumer's physical mail, email and text messages, unless the business is the intended recipient of the communication.
- A consumer's genetic data.
- Additionally, "sensitive personal information" means:
- The processing of biometric information processed for the purpose of uniquely identifying a consumer.
- Personal information collected and analyzed concerning a consumer's health.
- Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

New Rights

- **Right to Correct Information:** A consumer has the right to request that a business correct any inaccurate personal information.
- **Right to Limit Use and Disclosure of Sensitive PI:** A consumer has the right to limit the use and disclosure of their SPI to that "use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods and services."
- **Right to Access Information About Automated Decision Making:** A consumer has the right to request "meaningful information about the logic involved in those decision–making processes, as well as a description of the likely outcome of the process with respect to the consumer."
- **Right to Opt–Out of Automated Decision-Making Technology:** A consumer has the right to opt–out of being subject to automated decision–making processes, including profiling.

clarip

Amended Rights

- **Right to Opt–Out of Third-Party Sales and Sharing:** The CCPA allows consumers to opt–out of businesses selling their data. The CPRA expands this right to include the sharing of personal information, in addition to selling. The CPRA defines sharing as "disclosing, disseminating, making available, transferring, … a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration …"

Request the full white paper

Clarip takes enterprise privacy governance to the next level and helps organizations reduce risks, engage better, and gain customers' trust! Contact us at www.clarip.com or call Clarip at 1-888-252-5653 for a demo.

For more information contact sales@clarip.com

Mike Mango
Vice President of Sales
mmango@clarip.com
(646) 983-4618

clarip