CARTER/LEDYARD

our resources

California Expands Consumer Privacy Rights and Protections

February 12, 2021

While California was already well ahead of the curve with respect to privacy legislation, in November 2020, its voters enacted a new privacy law—the California Privacy Rights Act (the "CPRA"). The CPRA clarifies some aspects of California's existing privacy law framework known as the California Consumer Privacy Act (the "CCPA") and introduces a number of substantive changes designed to strengthen the privacy rights and protections for California residents.

The law appears to have been inspired, at least in part, by the European Union's General Data Protection Regulation (the "GDPR"). For companies already in compliance with the GDPR, complying with the CPRA will be a minor but necessary lift. For others that have not focused on privacy compliance, several additions under the CPRA render immediate action.

For background information about the requirements of the CCPA, see our previously published client advisory from January 2019.

Re-defined Scope of Covered "Businesses"

The CPRA modifies the threshold requirements for covered "businesses" that collect personal information about consumers. A for-profit entity doing business in California must meet one of the three amended thresholds to be considered a covered business under the CPRA (not-for-profit businesses do not fall within the scope of the law, as was the case with the CCPA):

- Must have ***at least $25 million annual gross revenue***, measured as of January 1st of the previous calendar year.
- The ***number of consumers or households*** from which a business annually buys, sells or shares personal information of consumers is increased to ***100,000*** (the threshold was 50,000 under the CCPA), eliminating many smaller businesses from the scope of the regulation. The calculation no longer includes reference to "devices", so households utilizing multiple internet-enabled devices will only be counted once. As with the CCPA, the definition of "consumer" includes a natural person who is a California resident.
- ***More than 50 percent of a business's annual revenue*** is derived from the disclosure of personal information, which includes ***both "selling" and "sharing" of personal information***. Under the CCPA, only "selling" was factored into this assessment. The CPRA extends to entities that control or are controlled by a covered business, share common branding with the business, and with which the business shares consumer's personal information.

The CPRA also extends obligations to joint ventures or partnerships in which a covered business has at least a 40% interest.

The CPRA extends the existing moratoria for certain personal information collected in the business to business "B2B" and employee data contexts to January 1, 2023.

Regulation of Behavioral Advertising

The CPRA amends the CCPA to regulate behavioral advertising that uses personal information to target California residents with marketing based on profiling.

The law accomplishes this by introducing the term "sharing" as a distinct activity from "selling" personal information. Sharing is defined as "disclosing or otherwise communicating a consumer's personal information for cross-context behavioral advertising." This includes ad targeting based on information obtained about a consumer across different apps or services—whether or not for monetary or other valuable consideration—and often involves transactions between a business and a third party. Since every obligation previously extended to "sales" under the CCPA now applies to "sharing", as defined in the CPRA, privacy policies should be updated to discuss the ways in which data is shared and explain the opt-out right.

New Category of "Sensitive Personal Information"

The CPRA creates a new category of personal information, called "Sensitive Personal Information", which includes the following: consumer identification numbers, such as Social Security number, driver's license number, state ID or passport number; financial information; account log-in credentials; precise geolocation data; racial and ethnic information; religious or philosophical beliefs; union membership; personal communications; genetic, biometric or health information; and information about sex life or sexual orientation.

Businesses must provide the following information to consumers at or before the collection point: (i) whether personal information is sold or shared; (ii) information about the collection, processing and disclosure of sensitive personal information; (iii) the length of time the business intends to retain the category of information, or, if not possible, the criteria used to determine such period.

Businesses must also provide a "*Limit the Use of My Sensitive Personal Information*" link on websites and/or mobile applications and enable consumers to limit the use and disclosure of sensitive personal information to a limited subset of purposes enumerated in the law. If this option is exercised by a consumer, businesses must limit the use of sensitive personal information to that which is necessary to perform services or provide goods reasonably expected by an average consumer and certain additional business purposes specified in the law, such as for product improvement or for security.

New and Expanded CCPA Rights

The CPRA creates a number of new rights and modifies certain existing rights of consumers under the CCPA:

- Right to correction: Consumers can request that their personal information or sensitive personal information be corrected if they find it to be inaccurate upon receiving results of their verifiable consumer request. This right mirrors the right to correct under the GDPR.

- Right to opt-out of automated decision-making: Consumers can refuse to allow companies to use their personal information or sensitive personal information gathered from targeted, behavioral advertisements online. Consumers can also request access to information about how automated decision technologies work and how their information is used.

- Right to limit use and disclosure of sensitive personal information: Consumers may limit the use and disclosure of sensitive personal information to that "which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods and services," subject to certain exemptions. Covered businesses must implement procedures to allow consumers to limit the use of sensitive personal information, such as through a clear link on a website or mobile app.

The five modified CCPA rights are:

- Right to delete: Companies must notify third parties (including service providers and "contractors," discussed below) to whom the business has sold or shared information if a consumer requests deletion of information.

- Right to know: For personal information collected on or after January 1, 2022, the CPRA allows a consumer to make a request to know beyond the CPRA's 12-month look-back period as long as doing so does not prove "impossible" or "involve a disproportionate effort." This expanded right does not require a business to keep personal information for any period of time.

- Right to opt-out: Consumers may opt out of the sale or sharing of their personal information, specifically for behavioral advertisements. Companies not currently providing opt-out rights for third-party behavioral advertising technologies must adopt processes to incorporate these opt-out procedures and must implement the "Do not Sell or Share my Personal Information" link across their web presence.

- Rights of minors: The affirmative opt-in requirement for the sale of information about minors is extended under the CPRA to include the sharing of personal information for behavioral advertising.

- Right to data portability: California residents can request to have their personal information transported to other businesses or organizations.

New Administrative Agency, the CalPPA

The CPRA creates a new administrative enforcement agency, the CalPPA, which has the administrative authority and jurisdiction to implement, audit and enforce the CCPA and the CPRA. Enforcement authority currently rests with the office of the California Attorney General. Consumers should expect greater oversight and more regulation with the creation of this dedicated agency.

Businesses may self-certify to the CalPPA that they are in compliance and agree to be bound by the terms of the law as a brand differentiator for compliant businesses.

Private Right of Action

The CPRA expands the private right of action for data breaches resulting from unreasonable security practices under the CCPA to also apply to the unauthorized access to or disclosure of consumer's unencrypted email address in combination with a password or security question and answer that would permit access to an account where reasonable security practices were not in place.

Additional Third-Party Obligations for Service Providers, Third Parties, and Contractors

The CPRA introduces the term "contractors," defined as persons to whom a business makes available a consumer's personal information for a business purpose pursuant to a written contract with the business. The law imposes new contractual obligations on this newly defined category in addition to service providers and other third parties, similar to the distinct obligations imposed on data processors under the GDPR. Any third-party agreements between businesses and service providers or contractors must prohibit the use of disclosure of personal information for any purpose other than the specific purpose identified in the contract, among other restrictions. If service providers and contractors contract with other entities to perform services, they must pass these contractual restrictions downstream.

Businesses should review and revise their contracts with service providers and contractors in order to ensure compliance with the CPRA.

When does the CPRA go into effect?

The CPRA will take effect on January 1, 2023 and the CCPA will remain in effect until then. However, there is a one-year lookback period for personal information collected starting on January 1, 2022.

Businesses should closely monitor subsequent rulemakings under the CPRA as the law grants the Attorney General, and subsequently the newly created CalPPA, the authority to issue regulations on a wide range of topics. The CPRA calls for final regulations to be adopted by July 1, 2022, one year before the CPRA becomes enforceable.

Conclusion

As data privacy laws continue to evolve in the United States, businesses should take stock now of what data they collect, adopt policies to ensure compliance with applicable laws, and update those policies currently in place.

Businesses are encouraged to consult legal counsel to assist in assessing whether they are subject to the CPRA and CCPA (or GDPR, or other applicable privacy law or regulation), interpreting the relevant provisions, and creating and implementing a privacy policy and strategy to ensure compliance.

* * *

related professionals

Matthew D. Dunn / Partner
D 212-238-8706
mdunn@clm.com

John M. Griem, Jr. / Partner
D 212-238-8659
griem@clm.com