GUIDANCE NOTE

California - Cookies & Similar Technologies

Mary Grieco
OLSHAN FROME WOLOSKY LLP



Morgan Spina
OLSHAN FROME WOLOSKY LLP



Rachel Gold
OLSHAN FROME WOLOSKY LLP



Last Updated: 15 hours ago

August 2026

1. Governing Texts

1.1. Legislation

The California Consumer Privacy Act of 2018 (last amended in 2020) (CCPA) creates consumer rights related to the collection, deletion, and sharing of personal information, including via cookies.

Sometime after enacting the CCPA, the California Attorney General (AG) published the California Consumer Privacy Regulations (the CCPA Regulations). The purpose of the CCPA Regulations was to establish procedures to facilitate

consumer rights under the CCPA and guide businesses with regard to compliance practices. Pursuant to the CCPA, the AG has been tasked with the bulk of enforcement responsibilities.

California subsequently amended the CCPA by enacting the California Privacy Rights Act of 2020 (CPRA) (consolidated version available here). The CPRA provisions became effective on January 1, 2023. In addition to expanding the CCPA, the CPRA created California's first agency focused solely on privacy issues, the California Privacy Protection Agency (CPPA). The CPRA tasked the CPPA with revising the CCPA Regulations. On September 23, 2025, the California Office of Administrative Law approved revised CCPA Regulations (Revised CCPA Regulation). The Revised CCPA Regulations took effect on January 1, 2026.

1.2. Regulatory Authority Guidance

The AG maintains a list of CCPA enforcement case examples as actions taken against companies since July 1, 2020, the first day CCPA enforcement began. The AG stated that it provided this information as "illustrative examples of situations in which it sent a notice of alleged noncompliance and steps taken by each company in response." In addition, the AG updated its CCPA frequently asked questions, and the CPPA released CCPA frequently asked questions. The Revised CCPA Regulations provide businesses with guidance on how to meet their obligations under the CCPA.

Finally, in September 2024, the CPPA issued Enforcement Advisory No. 2024-02 -Avoiding Dark Patterns: Clear and Understandable Language, Symmetry in Choice, which highlights the importance of avoiding dark patterns in consumer interfaces under the CCPA and includes examples of cookie banners whose user interfaces are considered compliant.

2. Definitions

Cookies & similar technologies: There is no definition of 'cookies' in the CCPA. However, cookies are included within the CCPA's definition of unique personal identifiers. In particular, §1798.140(aj) of the CCPA defines 'unique identifier' or 'unique personal identifier' as "a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, 'family' means a custodial parent or guardian and any minor children under 18 years of age over which the parent or guardian has custody."

Consent: §1798.140(h) of the CCPA includes a definition of 'consent,' namely "any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through the use of dark patterns does not constitute consent." The CCPA Revised Regulation clarifies that a cookie banner offering only "Accept All" and "More Information" (or "Preferences") is not symmetrical and constitutes a dark pattern; an equal choice would be "Accept All" and "Decline All". Additionally it states that "[a] consumer closing or navigating away from a pop-up window on a website that requests consent without first affirmatively selecting the equivalent of an "I accept" button shall not constitute consent."

Personal data: The CCPA defines 'personal information' as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or

could be reasonably linked, directly or indirectly, with a particular consumer or household:

- identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- any personal information described in §1798.80(e) of Title 1.81. of Part 4 of Division 3 of the California Civil Code (Cal. Civ. Code);
- characteristics of protected classifications under California or federal law;
- commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- biometric information;
- internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement;
- geolocation data;
- audio, electronic, visual, thermal, olfactory, or similar information;
- professional or employment-related information;
- education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act of 1974 (FERPA); and
- inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes (§1798.140(v)(1) of the CCPA).

Data processing: The CCPA defines 'processing' as "any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means" (§1798.140(y) of the CCPA).

Online identifiers: The CCPA references 'identifiers' as "a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers" (§1798.140(v)(1)(A) of the CPRA).

Sell/sale: 'Sell,' 'selling,' 'sale,' or 'sold," is defined as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration." (§1798.140(ad)(1) of the CCPA).

Share/shared/sharing: The CCPA defines 'share' as "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, 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, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged" (§1798.140(ah) of the CCPA).

Cross-context behavioral advertising: The CCPA defines 'cross-context behavioral advertising' as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interact" (§1798.140(k) of the CCPA).

Sensitive personal information: §1798.140(ae) of the CCPA defines 'sensitive personal information' 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 in combination 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, citizenship or immigration status, religious or philosophical beliefs, or union membership;
    - the contents of a consumer's mail, email, and text messages, unless the business is the intended recipient of the communication;
    - a consumer's genetic data; and
    - a consumer's neural data, which is defined as information that is generated by measuring the activity of a consumer's central or peripheral nervous system, and that is not inferred from nonneural information;
- the processing of biometric information 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; and
- personal information of consumers that the business has actual knowledge are less than 16 years of age. A business that willfully disregards a consumer's age shall be deemed to have had actual knowledge of the consumer's age.

3. Consent Management

3.1. Is consent required?

The CCPA does not require the use of cookies to be disclosed by a cookie banner. Furthermore, the CCPA does not require companies to obtain consent from consumers prior to the use of cookies. Companies are, however, required to disclose the use of cookies in their privacy policies.

Although companies are not required to obtain consent before placing cookies under the CCPA, it is a best practice to obtain consent before using third-party cookies for anything other than a "business purpose," such as for cross-context behavioral advertising purposes. By obtaining affirmative consent from consumers before placing analytics or marketing cookies by, for example, displaying a cookie banner that requires a consumer to affirmatively consent to the placement of cookies, a company may help mitigate some risk. This best practice has become increasingly important in light of recent litigation alleging that planting tracking cookies prior to obtaining user consent violates California's wiretapping laws, including the California Invasion of Privacy Act (Cal. Penal Code §§630 et seq.) (CIPA). These lawsuits allege that third-party tracking technologies, such as session replay software and advertising pixels, constitute unlawful interception of communications when deployed without prior consent. While these cases are still developing, businesses should be aware of this emerging litigation risk and consider implementing consent-first cookie practices to mitigate potential exposure under both the CCPA and CIPA.

Although prior express consent is not generally required under the CCPA, businesses are required to provide an opt-out for consumers regarding the sale of personal information or sharing of information as those terms are defined under the CCPA.

Further, the Revised CCPA Regulations include a section on Opt-Out Preference Signals (§7025 of the Revised CCPA Regulations). The Revised CCPA Regulations state that businesses that sell or share personal information must process opt-out preference signals that meet certain requirements as a valid request to opt-out of the sale/sharing of information. The Revised CCPA Regulations go on to state that a "notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to opt-out of sale/sharing because cookies concern the collection of personal information and not the sale or sharing of personal information" (§7026(a)(4) of the Revised CCPA Regulations).

Again, it is strongly recommended that businesses include an opt-in cookie banner popup as a best practice.

3.2. Conditions for valid consent

As noted above, express consent is not required for the placement of cookies under the CCPA. However, companies should recognize opt-out and 'Do Not Track' signals, including recognizing technologies like Global Privacy Control (GPC).

3.3. Analytics and audience measurement cookies

Please see the section above on conditions for valid consent.

3.4. Exemptions

Not applicable.

3.5. Cookie information requirements

The CCPA includes several notice, disclosure, correction, and deletion requirements. Specifically, the CCPA requires businesses to disclose what personal and sensitive personal information they collect, sell, share, or disclose, for what purposes it is selling or sharing such information, and its retention policies.

3.6. Cookie consent mechanism

The Revised CCPA Regulation provides that websites must display confirmation that an opt-out request has been processed. For example, websites may display text stating that the preference was honored or show a toggle indicating the consumer has opted out. The opt-out process must be at least as simple as the opt-in process.

3.7. Cookie walls

Not applicable.

3.8. Consent duration

Not applicable.

4. Cookies & Third Parties

4.1. Conditions for placement of third-party cookies

§1798.120 of the CCPA states that if a business 'sells' personal information to or 'shares' personal information with third parties, then the business "shall provide notice to consumers [...] that this information may be sold or shared and that consumers have the 'right to opt-out' of the sale or sharing of their personal information." A distinction is made between 'service providers' and 'third parties' within the CCPA.

Based on the definitions of 'personal information' and 'unique personal identifier' in the CCPA, the information collected by cookies may be considered 'personal information' under California law. Therefore, a business must determine if it is 'selling' or 'sharing' personal information if it allows a third party to collect information from consumers using cookies.

The CCPA's broad definitions of 'sale' and 'share' may, depending on the specific circumstances, such as for cross-context behavioral advertising, encompass situations where a company allows a third party to gather information from consumers through the use of cookies.

If a business allows a 'third party' to plant and/or collect personal information from cookies for a 'commercial purpose,' the business must allow the consumer the option to opt out of the use of such third-party cookies and the collection and use of personal information by the third party, as this would likely constitute a 'sale' of personal information to the third party. A 'commercial purpose' is defined broadly in §1798.140(g) of the CCPA as "to advance a commercial or economic interest, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchanger products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction."

In the event that a business allows a service provider or third party to track consumers using cookies or gather information using cookies from the business

website, this must be disclosed to consumers (usually in the website's privacy policy), and the categories of service providers and third parties with whom personal information is shared must be disclosed to a consumer in response to a verifiable request.

In addition, a business that 'sells' personal information to a third party or 'shares' personal information with a third party, through the use of cookies or otherwise, must provide a conspicuous notice to allow a consumer to opt-out of the same and must respond to a consumer request to opt-out.

4.2. Roles and responsibilities

The use of cookies on a website by a 'service provider' is generally not deemed a 'sale' of personal information, as long as the information collected by the 'service provider' is necessary to perform a 'business purpose' and the business and 'service provider' have entered into an appropriate agreement that contains certain provisions.

In this context, §1798.140(e) of the CCPA sets forth certain actions that would be deemed a 'business purpose,' namely:

- auditing interactions with consumers;
- security purposes;
- debugging/repair;
- certain short-term uses;
- performing services such as maintaining or servicing accounts, providing customer service, processing payments, providing certain advertising and marketing services, providing analytical services;
- providing advertising and marketing services (except cross-context behavioral advertising) to the consumer, as long as a service provider or contractor does not combine the personal information of opted-out consumers with the personal information that the business collected independently;
- internal research for tech development; and
- quality and safety maintenance and verification.

In addition, for a company to be deemed a 'service provider,' the company and the business must have a written agreement between them that contains certain clauses set forth in the CCPA and the Revised CCPA Regulations. Specifically, a 'service provider' must agree not to retain, use, or disclose personal information obtained in the course of providing services, except:

- to perform the services specified in the agreement;
- to retain and employ another service provider as a subcontractor (provided the subcontractor also enters into an appropriate service provider agreement);
- for internal use by the service provider to build or improve the quality of its own services;
- to detect security incidents or protect against fraudulent or illegal activity;
- to comply with applicable laws;
- to comply with a civil, criminal, or regulatory inquiry, investigation, or summons;
- to cooperate with law enforcement agencies concerning conduct that the business, service provider, or other, reasonably and in good faith, believes may violate applicable laws; or
- to exercise or defend legal claims.

The CPRA creates a new requirement for businesses that collect consumer personal information to execute written contracts containing specific provisions whenever it discloses that personal information to a service provider or contractor for a business purpose, or sells or shares the personal information with a third party (§1798.100(d) of the CCPA). The agreement must:

- specify that the personal information is sold or disclosed by the business only for limited and specified purposes;
- obligate the third party, service provider, or contractor to comply with applicable obligations of the CCPA and provide the same level of privacy protection as required under the CCPA;
- grant the business rights to take reasonable and appropriate steps to help ensure that the third party, service provider, or contractor uses the personal

information transferred in a manner consistent with the business's obligations under the CCPA;

- require the third party, service provider, or contractor to notify the business if it makes a determination that it can no longer meet its obligations under the CCPA; and
- grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

4.3. International data transfers

Not applicable.

5. Cookie Retention

There are no specific requirements or guidance regarding cookie retention.

6. Additional Information

The Revised CCPA Regulations require businesses to recognize GPCs, "such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information" as a valid request to opt-out pursuant to the CCPA. Specifically, it requires businesses to:

- display visible confirmation of GPC processing;
- not interpret the absence of a GPC signal as consent to opt back in; and

- meet detailed processing requirements if they wish to avoid posting separate opt-out links.

As such, based on the Revised CCPA Regulations, businesses are required to recognize 'Do Not Track' signals from browsers. This is further supported by the Sephora settlement (see the section on case law and enforcement decisions below).

7. Case Law & Enforcement Decisions

The AG reached a settlement with Sephora, Inc. regarding allegations that the company violated the CCPA. Among other requirements, the settlement states that Sephora must provide mechanisms for consumers to opt out of the sale of personal information, including via the GPC, and must ensure that its service provider agreements comply with the CCPA requirements.

The AG reached a settlement with Google resolving allegations that Google's privacy practices violated California laws. The AG's investigation found the Google was telling users that it would no longer track their location once they opted out, but that Google was actual continuing to track its users' movements for its own commercial gains. As part of the settlement, Google agreed to provide more transparency regarding location tracking and to show additional information to users when enabling location-related account settings.

The AG reached a settlement with DoorDash, resolving allegations that DoorDash violated the CCPA and CalOPPA. The AG determined that DoorDash sold its California customers' personal information without providing notice or an opportunity to opt out.

The CPPA fined Honda Motor Co., Inc. $632,000 for multiple violations of the CCPA, and as part of its corrective measures, the CPPA required Honda to include a link to manage cookie preferences within its privacy center, privacy

policy, and in the footer of privacy policy webpages, and include a 'reject all' button within the cookie management platform to provide symmetry in choice.

The CPPA fined Todd Snyder, Inc. $345,178 for failing to allow consumers to opt out of personal information sharing due to its Cookie Preferences Center being configured incorrectly.

The CPPA fined Tractor Supply Company $1.35 million for claims related to failure to timely process consumer requests, mishandling employment data and other CCPA violations.

The AG settled with Disney for $2.75 million related to failures to honor opt-out requests across its streaming platforms, including those made through GPC.

8. Penalties

Pursuant to §1798.155 of the CCPA, any business, service provider, or other person that violates the CCPA shall be subject to an injunction and a civil penalty of no more than $2,500 for each violation, or $7,500 for each intentional violation.

The CCPA also allows the CPPA to enforce the statute and any enacted regulations through administrative proceedings with corresponding administrative fines.

Topics: Cookies

Jurisdictions: United States (USA) Federal, California