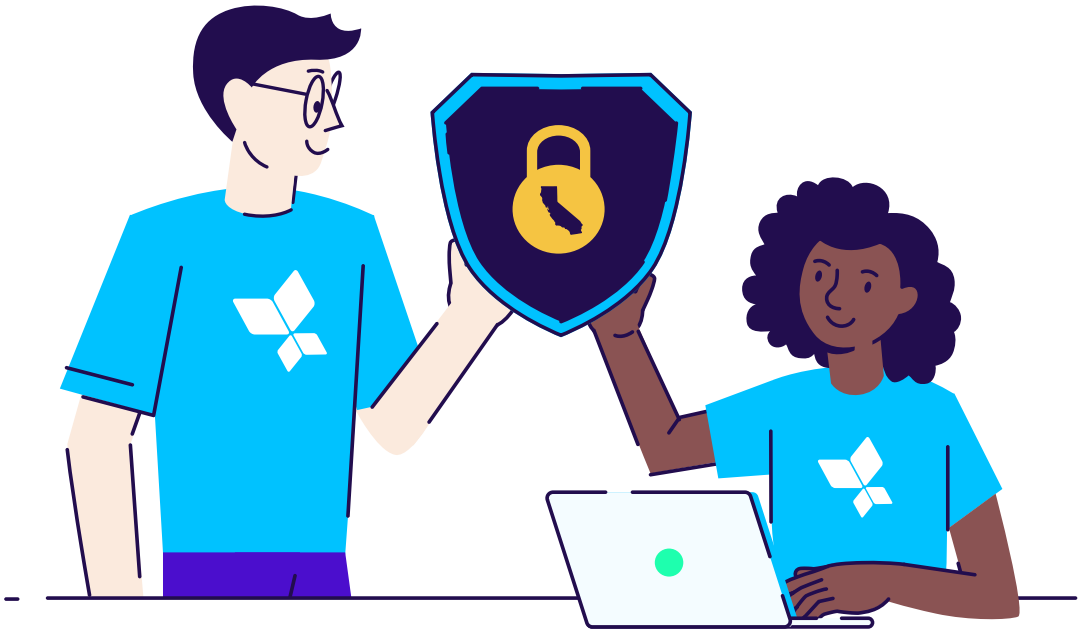
CCPA and other US state privacy laws



The California Privacy Rights Act and other U.S. State Law Updates

A word from our lawyers: Nothing stated here is legal advice. It is provided for your information and convenience. We strongly encourage that you work closely with legal and other professional advisors to determine exactly how the CCPA, CPRA and other State Laws apply to you.

Introduction and background

The world is becoming increasingly more private. In the last several years, laws and regulations have tightened on what organizations may and may not do with personal data.

The California Consumer Privacy Act (CCPA) originally took effect in 2020, aiming to provide the residents of California with similar rights as the GDPR provided citizens of the EU. The CCPA has since been amended by the California Privacy Rights Act (CPRA). The CPRA, effective January 1, 2023, increases the obligations of Businesses under the CCPA by providing Consumers with new privacy rights. Even for companies already compliant with the CCPA, the CPRA will require some adaptation, especially for those in the advertising industry.

As the industry's leading marketing measurement and analytics platform, AppsFlyer is committed to providing its customers full transparency and control over their users' personal data, empowering them in their pathway to regulatory compliance.

CCPA & CPRA: scope of application

Similar to the GDPR and other privacy laws, the CCPA/CPRA is intended to provide California consumers (including business professionals and employees) and households (devices with the same IP address) with increased control over their data and privacy while imposing increased obligations on businesses. In particular, several provisions are specifically designed to enable consumers to restrict the sale or 'sharing' of their personal information including identifiers commonly used by the ad tech ecosystem.

Under the CPRA, any form of behavioral targeting of website or mobile app visitors through ads on another website or app constitutes 'sharing'. In addition, the CPRA text makes any provider of services that directly supports cross-context behavioral advertising a "third party" under the law. This means that the website or app that 'shares' the identifier with the 'third party' to be used for behavioral advertising, must offer their users a distinct opt-out choice before sharing with that 'third party'. This opt-out must be honored by the website, app and 'third party' entity within forty-five (45) days of receipt.

Enforcement of the CCPA/CPRA will fall upon the Attorney General of California, together with a new regulatory body: the California Privacy Protection Agency.

Businesses

The CPRA has modified the CCPA's definition of a covered "Business." Now, the law applies to any for profit entity that does business in California, collects at least 100,000 unique CA-specific identifiers per calendar year (or if state geographic is unknown, estimated with at least 1,000,000 unique identifiers across the U.S. per year) and meets any of the following conditions:

- Has annual gross revenues in excess $25,000,000 (not just California revenue);
- Annually buys, receives, sells, or shares for commercial purposes, the personal information of 100,000 or more California consumers, households, or devices (which includes cookies, device or mobile advertising IDs and most IP addresses); or
- Derives 50 percent or more of its annual revenues from 'selling or sharing' consumers' personal information.

Under the CPRA, the scope of a 'service provider' has been left unchanged. The CPRA has, however, added the concept of a 'contractor', which still remains largely to be elaborated upon by the Californian regulator and for now has been designated as "a person to whom the business makes available a consumer's personal information for a business purpose".

Consumers

The CCPA/CPRA applies to personal information of Consumers, defined broadly as follows: "any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household".

Examples include:

- Name pseudonym, or alias
- Postal address, email address, phone number (and quite possibly - fax numbers)
- Any unique identifiers, including cookie IDs, device IDs, and mobile advertising IDs
- IP address
- Government-issued ID numbers, including drivers license or social security numbers
- Behavioral or commercial records, including products or services purchased or considered purchasing
- Biometric information, including photos used to identify an individual
- Browsing and search history, including interactions with mobile applications and advertisements associated with an individual
- Any geolocation data associated with an individual or household
- Professional or employment-related information, including titles or roles

Sharing of information

The CCPA focused on the 'sale' of personal information. The CPRA introduces the term 'sharing' for cross-context behavioral advertising purposes and ensures that California consumers can opt-out of any sharing of their personal information for profile-based ad targeting across sites and apps. As a result of this change, all businesses that enable ad targeting across the web or app ecosystem are now required to either suppress anyone who has opted out, or pass along opt-out identifiers for their intermediaries to suppress against when attempting to target individual ads.

AppsFlyer doesn't 'sell' or 'share' personal data as defined under the CCPA/CPRA, nor does it combine personal information received from our customers with information received on behalf of another person, unless as required for us to provide the services as permitted under the CCPA. Using AppsFlyer therefore does not contribute to the notion of 'selling' or 'sharing' by advertisers.

Furthermore, and importantly, AppsFlyer does not perform 'cross-context behavioral advertising' and therefore maintains its role as a 'service provider' under the CCPA/CPRA.

Consumer Rights under the CCPA and CPRA

The CCPA provided consumers with certain rights. The CPRA expands those rights as further described below:

CCPA Rights:

- Right to Know
- Right to Access
- Right to Delete
- Right to Opt Out of the 'Sale' of Personal Information
- Right to Non-discrimination for Exercising these Rights

CPRA Rights:

- Right to Correct personal information

- Right of Opt Out of 'Sharing' for cross-context behavioral advertising purposes. "Sharing" is defined by the CPRA as the transfer or making available of a "consumer's personal information by the business to a third party explicitly for cross-context behavioral advertising (CCBA), whether or not for monetary or other valuable consideration." Cross-context behavioral advertising is defined 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 interacts."

- Right to Limit the Use and Disclosure of Sensitive Personal Information. Sensitive Personal Information is defined as (1) SSN; (2) drivers license; (3) state ID; (4) passport/passport number; (5) account login information, financial account, debit card, or credit card in combination with any required security or access code, password, or credentials allowing access; (6) precise geolocation; (7) racial or ethnic origin; (8) religious or philosophical beliefs; (9) union membership; (10) contents of consumers mail, email, and text messages unless sent to the Business; (11) personal information regarding sex life or sexual orientation; and (12) genetic data, biometric information used for identifying the individual, and personal information collected and analyzed concerning a consumer's health.

Enforcement under the CCPA/CPRA

Organizations found in violation of the CCPA/CPRA will be charged a penalty by either the California Attorney General or the California Privacy Protection Agency.

Penalties are:

- $2,500 for each violation
- $7,500 for each intentional violation

Don't be fooled by these seemingly low numbers; a violation will likely occur per consumer and these fines may easily reach millions for intentional violations. Under the CPRA there is no cure period for companies.

Consumers have a private right to action in certain cases where their unencrypted or unredacted personal information has been exposed due to a business's failure to maintain reasonable security safeguards. The CPRA expands this right by allowing consumers to bring lawsuits against a company if an email address in combination with a password or security question and answer is subjected to unauthorized access as a result of a company's unreasonable security procedures. While the scope is more limited, individuals may seek statutory damages between US$100 to US$750 dollars per violation which may be brought in class action claims.

Those apps separately collecting precise geolocation must now also disclose this as it is considered 'sensitive personal information' under the CPRA. They must therefore offer to 'Limit the Use of My Sensitive Information' with a link to enable an opt-out for their app users. App developers need to ensure that any such data is suppressed with any entities processing this data on their behalf, or for their own purposes.

Guide to compliance in respect of using AppsFlyer:

To contribute to your general compliance, it is recommended that customers falling under the CPRA provide Consumers with an enhanced privacy policy and be ready to link a 'Notice at Collection' reference to the relevant section of the privacy policy as prescribed by the CCPA. Mobile apps furthermore need to disclose the use of MMPs in general.

Businesses will also need to enable compliance with the new privacy rights under the CPRA for modification of personal information, and opt-out of the 'sale or share' of personal information. The latter can be accomplished by updating your homepage to include a "Do Not Sell or Share My Personal Information" link which leads to an opt out i. The website can also include a "Limit the Use and Disclosure of My Sensitive Personal Information" -link, if applicable, which should lead to an opt out for using and disclosing sensitive personal information. Alternatively, implement a one single link which leads to both opt outs with a 'Your Privacy Choices' link.

We want to note that the nature of the data AppsFlyer needs to receive in order to provide the services does not include any sensitive or direct personal information and is limited to personal data that is pseudonymised by nature (e.g. advertising device ID or IP address). It is in fact contractually prohibited to send AppsFlyer any sensitive personal information.

What about other U.S. State laws?

In addition to the CPRA, four more comprehensive U.S. state privacy laws come into effect in 2023 (1. The Virginia Consumer Data Protection Act - effective January 1, 2023; 2. The Colorado Privacy Act - effective July 1, 2023; 3. The Connecticut Data Privacy Act - effective July 1, 2023; and 4. The Utah Consumer Privacy Act). The following is a brief overview of such laws as they relate to targeted advertising, opt-out mechanisms and sensitive information.

Targeted advertising

Similar to the CPRA which provides consumers the right to opt out of the sharing of their personal information for the purpose of cross-context behavioral advertising, Virginia, Colorado, Connecticut, and Utah all provide consumers with the right to opt out of targeted advertising. Each of these laws largely defines targeted advertising the same (see table below) the only key difference being that Colorado and Connecticut explicitly include the use of inferred data in their definitions

Like California, each of these laws require that companies provide the ability to opt out of targeted advertising on a company's website.

	Definition of Targeted Advertising
CPRA	Called 'sharing' Sharing means "communicating orally, in writing, or by electronic or other means, a consumer's personal information . . . to a third party for cross-context behavioral advertising (CCBA), whether or not for monetary or other valuable consideration" CCBA means "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 interacts."
VCDPA	Displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. Targeted advertising does not include: 1. Ads based on activities within a controller's own websites or online applications; 2. Ads based on the context of a consumer's current search query, visit to a website, or online application; 3. Ads directed to a consumer in response to the consumer's request for information or feedback; or 4. Processing personal data processed solely for measuring or reporting advertising performance, reach, or frequency

	Definition of Targeted Advertising
CPA	Displaying to a consumer an advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict consumer preferences or interests; Targeted advertising does not include: 1. Advertising to a consumer in response to the consumer's request for information or feedback; 2. Ads based on activities within a controller's own websites or online applications; 3. Ads based on the context of a consumer's current search query, visit to a website, or online application; or 4. Processing personal data solely for measuring or reporting advertising performance, reach, or frequency.
CTDPA	Displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests. Targeted advertising does not include: 1. Ads based on activities within a controller's own Internet web sites or online applications; 2. Ads based on the context of a consumer's current search query, visit to an Internet web site or online application; 3. Ads directed to a consumer in response to the consumer's request for information or feedback; or 4. Processing personal data solely to measure or report advertising frequency, performance or reach.

	Definition of Targeted Advertising
UCPA	Displaying an advertisement to a consumer where the advertisement is selected based on personal data obtained from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests. Targeted advertising does not include advertising: 1. based on a consumer's activities within a controller's website or online application or any affiliated website or online application; 2. based on the context of a consumer's current search query or visit to a website or online application; 3. directed to a consumer in response to the consumer's request for information, product, a service, or feedback; or 4. processing personal data solely to measure or report advertising: (A) performance; (B) reach; or (C) frequency.

Universal opt out mechanisms

The CPRA requires businesses to honor universal opt out mechanisms for the opting out of the sale or share of personal information (called "Opt-Out Preference Signals." Similarly, Colorado requires businesses honor such universal opt out mechanisms for the sale of personal information and for targeted advertising. Specifically, from July 1, 2023 (when the CPA goes into effect) until July 1, 2024, controllers that process personal data for targeted advertising or sales may allow consumers to opt out of such processing through a user-selected universal opt-out mechanism. Effective July 1, 2024, controllers are required to allow consumers to opt out. As for Connecticut, universal opt-out mechanisms must be recognized by controllers as valid consumer requests beginning January 1, 2025. While Virginia and Utah don't explicitly contemplate universal opt out mechanisms, rulemaking has not finished in these states and it is possible that future rulemaking will require honoring such opt outs.

Sensitive information

To add to the complexity, Virginia, Colorado, and Connecticut all require prior, opt-in consent from consumers before the use of sensitive information - each law has a slightly different definition of sensitive information (see table below). For companies that rely on sensitive information, these opt-in consent requirements for processing have a large impact. It should also be noted that the use of sensitive information collected by a company prior to the effective date of these laws, still requires consent. Practically speaking, in order for a business to use sensitive information they already have on Virginians, Coloradans, and Connecticutians, it must first obtain these consumers' consent.

Utah takes a different approach, it simply requires companies to provide consumers with the ability to opt out of the collection and use of sensitive information. Unlike for the CPRA, this opt out does not have to be granular.

	Consent for Sensitive Information	Definition of Sensitive Information
CPRA	Opt out (with the right to "limit use and disclosure of sensitive information")	Definition: (1) SSN; (2) drivers license; (3) state ID; (4) passport/passport number; (5) account login information, financial account, debit card, or credit card in combination with any required security or access code, password, or credentials allowing access; (6) precise geolocation; (7) racial or ethnic origin; (8) religious or philosophical beliefs; (9) union membership; (10) contents of consumers mail, email, and text messages unless sent to the Business; (11) personal information regarding sex life or sexual orientation; and (12) genetic data, biometric information used for identifying the individual, and personal information collected and analyzed concerning a consumer's health.

	Consent for Sensitive Information	Definition of Sensitive Information
VCDPA	Opt in	Definition: (1) precise geolocation; (2) personal data collected from a known child; (3) racial or ethnic origin; (4) religious beliefs; (5) sexual orientation; (6) citizenship or immigration status; (7) mental or physical health diagnosis; (8) genetic or biometric data for the purpose of identifying an individual.
CPA	Opt in	Definition: (1) personal data collected from a known child; (2) racial or ethnic origin; (3) religious beliefs; (4) sexual orientation; (5) information regarding an individual's sex life; (6) citizenship or immigration status; (7) mental or physical health diagnosis and conditions; (8) genetic or biometric data for the purpose of identifying an individual.
CTDPA	Opt in	Definition: (1) racial or ethnic origin; (2) religious beliefs; (3) mental or physical health condition or diagnosis; (4) sex life; (5) sexual orientation; (6) citizenship or immigration status; (7) personal data from a known child; (8) precise geolocation data; and (9) genetic or biometric data for the purpose of identifying an individual.

	Consent for Sensitive Information	Definition of Sensitive Information
UCPA	Opt out	Definition: personal data that reveals an individual's (1) racial or ethnic origin; (2) religious beliefs; (3) sexual orientation; (4) citizenship or immigration status; or (5) medical history, mental or physical health, medical treatment or diagnosis by a health care professional, plus specific geolocation data and certain genetic personal data or biometric data, all subject to limited exceptions.

Future compliance?

This evergrowing patchwork of US privacy laws has created a compliance hurdle for businesses, which increasingly are calling for a federal privacy law. And while there has also been significant momentum around the passing of a comprehensive federal privacy law in the U.S., no such law has passed to date. Because of this, businesses should expect more privacy laws to be passed in the U.S. in the coming years.

In the meantime, customers can feel confident that AppsFlyer will continue to provide solutions that will enable them to be compliant with US State laws and other global laws. Besides AppsFlyer operating as a service provider and not using the personal data for any reason other than to provide the services requested by our customer, AppsFlyer provides a DPA to cover its processing of the personal data. The DPA covers a range of issues such as AppsFlyer's commitment to implement appropriate technical and organizational measures to protect personal data, to assist customers with their compliance needs including by cooperating in respect of data protection impact assessments, individual rights request (such as the right of deletion), breach notification requirements and more. Lastly and generally, customers will need to also assess any additional laws applicable to them given their own products since certain unique industry specific obligations may apply to them in addition to the CPRA.