osano

A GUIDE TO CALIFORNIA'S CROWDED PRIVACY LANDSCAPE

TABLE OF CONTENTS

California gets a lot of press for its heavy-handed regulatory environment, but as the number one state in the Union by population and by GDP, it's got a lot to manage. There is no shortage of consumers in need of protection and businesses seeking a way to gain an edge in the competitive California economy.

The California regulatory landscape is crowded, and it can be easy to get lost. Use this guide to some of the Golden State's most significant privacy laws to get your bearings.

CALIFORNIA PRIVACY: AN OVERVIEW

When it comes to California privacy, the first set of laws to come to mind is the California Consumer Privacy Act (CCPA) and its update, the California Privacy Rights Act (CPRA; as the CPRA is the most recent piece of privacy legislation in California, we'll default to referring to the CPRA only from now on). These omnibus privacy bills give the broadest protection to consumers' privacy rights, but they aren't the only privacy bills in California by far.

Rather, the CPRA can be thought of as a set of laws that explicitly focus on Californians' fundamental right to privacy. Many of California's other privacy-related laws focus on specific aspects of privacy and particular applications of privacy protections, including:

- The California Age-Appropriate Design Code Act, which focuses on children's privacy
- CalOPPA, which is primarily concerned with businesses' privacy policies
- The Shine the Light Law, which regulates how organizations share their consumers' personal information with third parties involved in direct marketing
- The California Financial Information Privacy Act, which regulates how financial institutions collect and share consumers' personal information
- The California Invasion of Privacy Act, which prohibits wiretapping, tracking individuals' locations, eavesdropping, and the like

Collectively, these laws make California the most privacy-conscious state in the Union and one of the more privacy-conscious jurisdictions in the world.

Adhering to all, most, or even just one of these laws might seem like a challenge. Compliance can be complex, but to protect your brand and respect consumer rights, it's essential to dedicate energy and resources toward understanding and implementing your privacy program. The first step is learning what your obligations are. Let's review each of the major privacy laws at play in California and their requirements for businesses, starting with what is perhaps the most significant: The CPRA.

THE CCPA/CPRA

What is it?

The California Consumer Protection Act (CCPA) came into force in 2018 and was swiftly followed by the California Privacy Rights Act (CPRA), which, in turn, is effective on January 1, 2023. It amended the CCPA by clarifying certain misconceptions and strengthening certain provisions.

Together, these comprehensive privacy bills regulate many Californian and non-Californian businesses, obligating them to treat consumers' personal information in a thoughtful and respectful manner. In essence, these laws hinge on the concept of consent: Businesses must gain a consumer's consent before they can collect and process their data. If that consent is withdrawn, businesses must act accordingly.

Who does it apply to?

The CPRA applies to for-profit organizations that do business in California, collect the personal data of Californians, or have personal data collected for them, and fit one or more of these criteria:

- Buy, sell, or share the personal information of 100,000 California users or households.
- Create 50% or more of their revenue through the selling or sharing of personal information.
- Had $25 million in gross revenue in the preceding calendar year (e.g., January 1, 2022, to December 31, 2023, to start, and then from Jan. 1 to Jan. 1 after that).

What are its main requirements?

There is a lot to understand about the CPRA—it merits its own ebook to dive into all the specifics. Here are a couple of highlights:

Privacy policies

For one, businesses need to disclose a significant amount of information to consumers in their privacy policies (or in a conspicuous location on their websites). This includes:

- A description of the consumer's rights
- Two or more methods for submitting data subject access requests (DSARs), one of which must be a toll-free number
- The categories of personal information the business collects
- Whether the business sells/shares personal information and to whom
- And much more

Consent preferences

Businesses also have to honor consumers' consent preferences regarding personal information collection. For the most part, California is an opt-out jurisdiction. That means consumers are considered to have given consent to data collection if they have been notified (via the disclosures described above) and if they choose to continue to use the website, application, or another service. However, businesses must give consumers a means of opting out of that data collection. Typically, consumers can do so by submitting a DSAR.

DSARs

DSARs are requests that consumers make to exercise the rights protected by the CPRA and other data privacy laws. Businesses have to honor them if they want to be compliant. One of those DSAR rights is the ability to opt-out of data collection, but the CPRA specifies other privacy rights, including:

- The right to access, delete, and correct information: Consumers can ask to see what data you collect from them, and they can request to delete or update that data. Notably, the CPRA requires you to collaborate with any third parties you've shared that consumer data with, which can be tricky to handle if you aren't prepared.
- The right to object to sale or share: This right allows consumers to opt-out of the selling or sharing of their information. A "DO NOT SELL OR SHARE MY PERSONAL INFORMATION" link is required on your business's website, but a "Do Not Sell or Share" request must be honored however it is made.

- The right to opt-out of behavioral profiling and automated decision-making: Consumers can ask you to stop profiling and serving ads based on behavior, and they can ask you not to use automated decision-making to provide them with offers, products, services, etc.
- Right to object to the use of sensitive personal information: The CPRA includes a category of personal information defined as especially sensitive. The categories of "sensitive information" are discussed in detail later in this document. Consumers can ask you to limit the use of this data to only what is strictly necessary for your website to function (e.g., if you ran a genetic testing company, you would need a consumer's genetic data to provide your service). The CPRA also requires you to have a prominent button or link people can use to "limit the use of my sensitive personal information."
- Right to data portability: In essence, you must provide a consumer with their data in a structured, commonly used, machine-readable format so the data may be transferred to another company or entity.

Purpose limitation & data protection

The CPRA also requires purpose limitation, meaning that data should only be used for the purpose for which it was originally collected. This pairs with the CPRA's storage limitation requirements, which indicate that data should be deleted once that purpose has been fulfilled.

Additionally, businesses must take reasonable and appropriate security measures to protect data based on its sensitivity and potential for harm.

Personal information & data sharing

There are some strict requirements for the sharing of personal information. Personal information may only be shared with third parties for limited and specified purposes and only under a written agreement that requires the third party to protect the information as required by California law, regardless of where the third party is located.

While setting up these contracts can be time-consuming, a standard data processing agreement can be used for all third parties. In addition, data sharing under a data processing agreement may be done without the consumer's consent and may still be done if the consumer has made a "Do Not Sell or Share" request.

What penalties are associated with breaking the law?

The Attorney General's office and the newly created California Privacy Protection Agency (CPPA) have the power to investigate, and levy penalties on businesses they find are out of compliance.

Those penalties are:

- $2,500 per violation
- $7,500 for any willful violation involving the personal information of children under the age of 16.

Each person affected in a violation constitutes an "offense," so the fines can add up quickly.

What's unique about the law?

Quite a bit.

For one, the CPRA permits employees to make DSARs, which makes it unique among American state privacy laws. Businesses gather more and more sensitive personal information from their employees, and employees are more likely to make DSARs out of dissatisfaction (e.g., "Why was I let go? I'll make a DSAR and find out. Maybe they did something illegal, and I can sue").

For another, it's the only state privacy law with its own enforcement agency: The CPPA. Most state laws are enforced by the Attorney General, meaning that limited resources are available to go after businesses that violate the law. Not so in California; the CPPA and the Attorney General will enforce the CPRA and have plenty of time and funding to do so.

The CPRA also introduces the concept of sensitive personal information. This is data that could have an outsized impact on an individual if leaked or supplied to the wrong individuals. This includes:

- Ethnicity/racial origin
- Health conditions or diagnoses
- Sexual orientation
- Citizenship status
- Genetic/biometric information
- Precise Geolocation
- Email content
- Financial information
- Social security numbers and other forms of ID
- Religious or philosophical beliefs
- Trade union membership

THE CALIFORNIA AGE-APPROPRIATE DESIGN CODE ACT

What is it?

This law expands upon several existing minor protection laws, including California's Parent's Accountability and Protection Act and the federal Children's Online Privacy Protection Act (COPPA). However, the California Age-Appropriate Design Code Act (or CAADCA) serves as an updated, modern version of these laws that accounts for the new ways children interact with digital services.

In essence, it requires businesses whose services, products, or features are likely to be accessed by children to enact strict levels of protection, such as defaulting to the highest level of privacy settings, providing additional disclosures, conducting assessments to analyze privacy risk, and more.

Who does it apply to?

Under this law, any business that is also subject to the CPRA and provides an online service, product, or feature "likely to be accessed by children" under 18 would be subject to regulation.

What does it mean for a service, product, or feature to be "likely to be accessed by children"? The law defines this as:

- It is directed to children, as defined by the federal Children's Online Privacy Protection Act.
- It is routinely accessed by a significant number of children
- It has advertisements marketed to children
- It is substantially similar to, or the same as, an online service, product, or feature routinely accessed by a significant number of children
- It has design elements that are known to be of interest to children (such as games, cartoons, celebrities who appeal to children, and the like)

What are its main requirements?

Under CAADCA, businesses must:

- Default to the highest level of privacy settings unless the business can demonstrate that a different setting is in the child's best interest.
- Provide privacy information using clear language tailored to the likely age of children accessing the product or service.
- Conduct a Data Protection Impact Assessment (DPIA) before offering any new product or service. It's important to keep this DPIA on hand to provide to the Attorney General if they ask to see it; otherwise, the business is noncompliant.
- Estimate the age of child users with a reasonable level of certainty.
- Provide a clear signal to children if and when they are being monitored if the product or service permits parents or guardians to monitor the child's activity.
- Enforce privacy policies.
- Provide tools to help children (or their parents or guardians) exercise their privacy rights and report concerns.

CAADCA also features language around purpose limitation. Businesses cannot use a child's personal information for any reason beyond that for which it was originally collected, unless the organization can demonstrate a compelling reason why that additional purpose is in the child's best interest.

Additionally, businesses are prohibited from using personal information in a way that it knows is detrimental to the child's well-being.

Finally, CAADCA restricts the use of dark patterns (i.e., manipulative design practices); profiling; and the collection, sale, or sharing of a child's geolocation data.

What penalties are associated with breaking the law?

Like many U.S. privacy laws, enforcement is left in the hands of the Attorney General's office. If the Attorney General finds that a business has been working toward compliance with CAADCA but unintentionally violated the act, they may issue a 90-day cure period to allow the organization to address the violation.

If they fail to address the violation within that window or don't appear to be striving toward compliance, the business may be fined $2,500 per affected child if the violation is merely negligent. If the violations are intentional, the fines can be as high as $7,500 per child.

What's unique about the law?

CAADCA was actually modeled after the UK's Age-Appropriate Design Code, so it isn't exactly a COPPA 2.0 (that legislation is still in the works). While COPPA defines a child as anyone under the age of 13, CAADCA sets the threshold as the age of 18, making it much broader than COPPA.

Additionally, CAADCA established the California Children's Data Protection Working Group, which is tasked with determining the best methods for implementing the act. The working group is to identify which services, products, or features are likely to be accessed by children; ensure that age-assurance methods used by businesses are proportionate, protect privacy, and are minimally invasive; and evaluate the best way for the CPPA to work with the Department of Justice. If you suspect your organization is subject to CAADCA, it's a good idea to keep an eye out for any news from this working group.

CALIFORNIA ONLINE PRIVACY PROTECTION ACT

What is it?

Enacted in 2004, the California Online Privacy Protection Act (CalOPPA) was the first law in the nation to require websites to display their privacy policies conspicuously and for the owners or operators of those websites to comply with what they state in their privacy policy.

Who does it apply to?

Unlike the CPRA, CalOPPA applies to any business that collects and maintains the personally identifiable information of any California resident. It doesn't have to be 100,000 California residents; it can be just one.

Internet service providers and similar organizations that merely transmit or store data on behalf of a third party are exempt from CalOPPA, but pretty much any other digital channel is fair game. That includes commercial websites and mobile applications as well.

What are its main requirements?

Essentially, CalOPPA requires businesses to conspicuously post a privacy policy on their websites, convey specific information in that policy, and actually do what it says in the policy.

A privacy policy is considered "conspicuously" posted if it is shown on the homepage or if the homepage contains a link in a distinct type, font, or color; contains the word "privacy;" and directs the user to the privacy policy.

That privacy policy must contain:

- A list of the categories of personally identifiable information the website collects
- The categories of third parties with whom the website shares personally identifiable information
- How consumers can review and request changes to their collected information
- How the business will notify consumers of changes to their privacy policy
- The policy's effective date
- How the website responds to global Do Not Track signals
- Whether third parties collect visitors' personal information when using the website

What penalties are associated with breaking the law?

CalOPPA violations come with a maximum $2,500 fine per violation, although the Attorney General does provide a 30-day window to post a compliant privacy policy.

What's unique about the law?

CalOPPA was the first law in the U.S. to mandate privacy policies, and its scope is vast—virtually any website might process the personally identifiable information of a California resident. As a result, it's had an outsized impact on the internet as a whole. Nowadays, privacy policies are just something you do by default, thanks in part to CalOPPA.

SHINE THE LIGHT ACT

What is it?

Coming online in 2005, the Shine the Light (STL) Act is an early attempt by the California legislature at increasing transparency around businesses' data privacy practices. There is a great deal of overlap between the STL and the CPRA. While the CPRA is a more comprehensive, effective data privacy law, the STL is still an active part of the California data privacy regulatory landscape.

Who does it apply to?

Any business that has an established personal, family, household, or business relationship with a California resident and that discloses that consumer's personal information to a third party for direct marketing purposes must comply with the STL Act.

What are its main requirements?

Under the STL Act, businesses must disclose what personal information they've shared with third parties upon a consumer's request and which third parties received personal information. Consumers can also opt out of having their personal information shared with third parties for direct marketing purposes.

What penalties are associated with breaking the law?

If a business doesn't honor a consumer's request, it may be fined up to $500 per violation and up to $3,000 per willful, intentional, or reckless violation, as well as attorney fees and costs.

What's unique about the law?

It clearly overlaps with the CPRA's DSAR requirements. One of the criticisms around the STL Act was that it was difficult for consumers to exercise their rights and actually make requests, which is one reason why the CPRA reintroduced the concept of DSARs. Because the STL Act is still active, a business subject to the CPRA that fails to honor consumer DSARs could conceivably be fined twice; once for violating the CPRA and once for violating the STL.

CALIFORNIA FINANCIAL INFORMATION PRIVACY ACT

What is it?

The California Financial Information Privacy Act (CFIPA) requires financial institutions to obtain California consumers' consent before sharing their personal information with a third party and to disclose how they share that information.

Who does it apply to?

Any financial institution that does business in the state of California serving California residents is subject to the CFIPA.

What are its main requirements?

The CFIPA regulates how financial institutions handle non-public personal information (defined as any personally identifiable financial information, including whether an individual is a customer of or has obtained services from a financial institution).

The CFIPA prohibits financial institutions from selling or sharing non-public personal information with unaffiliated third parties without explicit written consent from the consumer. Information may be shared with affiliated organizations without opt-in consent, but the financial institution must clearly notify consumers that their information may be shared and allow them to opt out of such sharing. (NOTE: Enforcement of the prohibitions against sharing with affiliated entities has been permanently enjoined by the U.S. District Court for the Eastern District of California, as they were ruled to be preempted by federal law.)

Non-public personal information may be shared without consent in certain circumstances, such as:

- In response to law enforcement requests, subpoenas, requests from government regulators, and to fulfill other legal obligations.
- In connection with investigations of elder or dependent adult financial abuse.

- In connection with a merger, sale, or transfer of assets of the financial institution.
- To an entity performing necessary services on behalf of the financial institution, if a written contract is in place which prohibits the entity from using the information for any purpose other than for providing the contracted service.

Non-public personal information shared with a contracted service provider must be limited to only information necessary to provide the service.

Finally, a financial institution cannot discriminate against consumers that exercise their rights under CFIPA.

What penalties are associated with breaking the law?

There are a variety of agencies that enforce CFIPA. Depending on the nature of the financial institution, enforcement may come from the California Department of Financial Protection and Innovation, the Department of Insurance, or the California Attorney General.

Financial institutions that negligently expose a consumer's nonpublic personal information are subject to a $2,500 penalty per violation. If more than one individual's information is exposed, the total fine is capped at $500,000. The base fine remains the same for intentional violations, but there is no cap. And if the violation results in identity theft, all fines are doubled.

What's unique about the law?

Sometimes, data privacy laws will feature exceptions for financial institutions since the sensitive nature of their industry merits its own tailored regulations. The CFIPA serves as that tailored regulation in California, but the CPRA does not carve out the financial industry as a whole. So, California financial institutions are subject to both the CFIPA and the CPRA, increasing their risk.

CALIFORNIA INVASION OF PRIVACY ACT

What is it?

The California Invasion of Privacy Act (CIPA) grants California citizens protections against wiretapping and eavesdropping.

Who does it apply to?

This law protects all persons in the state of California, and therefore, any business interacting with somebody within California (whether they're a resident or not) may be subject to the law.

What are its main requirements?

CIPA protects the communications of individuals in California against:

- Wiretapping
- Eavesdropping
- Recording confidential communications without all parties' consent
- Monitoring or recording subscribers without written consent by cable and satellite TV businesses
- The use of electronic tracking devices

What penalties are associated with breaking the law?

The CIPA provides a private right of action. Plaintiffs may sue for up to $5,000 per violation and three times the amount of actual damages.

What's unique about the law?

While the law notably prohibits companies, individuals, and government agencies from recording communications, it also prohibits the use of tracking devices—given the proliferation of smartphones these days, businesses that track users' geolocation can run afoul of this law if they're not careful about compliance. In fact, that's exactly what happened to Apple in November of 2022.

...And many more

The California privacy landscape is crowded—too crowded to exhaustively list every privacy law it has on the books. This ebook has covered some of the significant laws that a typical business might need to be aware of, but individual organizations might have to contend with numerous other laws focused on the granular aspects of their industry.

Individuals interested in learning about the full scope of data privacy in California should visit the Attorney General's webpage on privacy laws, which covers both the state and federal laws at play in California.

But if you're more interested in taking a deep dive into perhaps the most significant California privacy law—the CPRA—you'll be best served by consulting our ebook, Prepare for California's next big privacy law: The CPRA. In it, we dive deeper into the CPRA specifics that are out of this guide's scope.

Access your free copy of "Prepare for California's next big privacy law: The CPRA" today

Download it now

@osano
linkedin.com/company/osano
http://facebook.com/osanoatx
osano.com

About Osano

Osano is a complete data privacy platform trusted by thousands of organizations around the world. Its platform simplifies compliance for complex data privacy laws such as GDPR, CCPS, LGPD, and more. Features include consent management, subject rights management, data discovery, and vendor risk monitoring. Osano is the most popular cookie compliance solution in the world, used on over 900,000 website to capture consent for more than 2.5 billion monthly visitors.