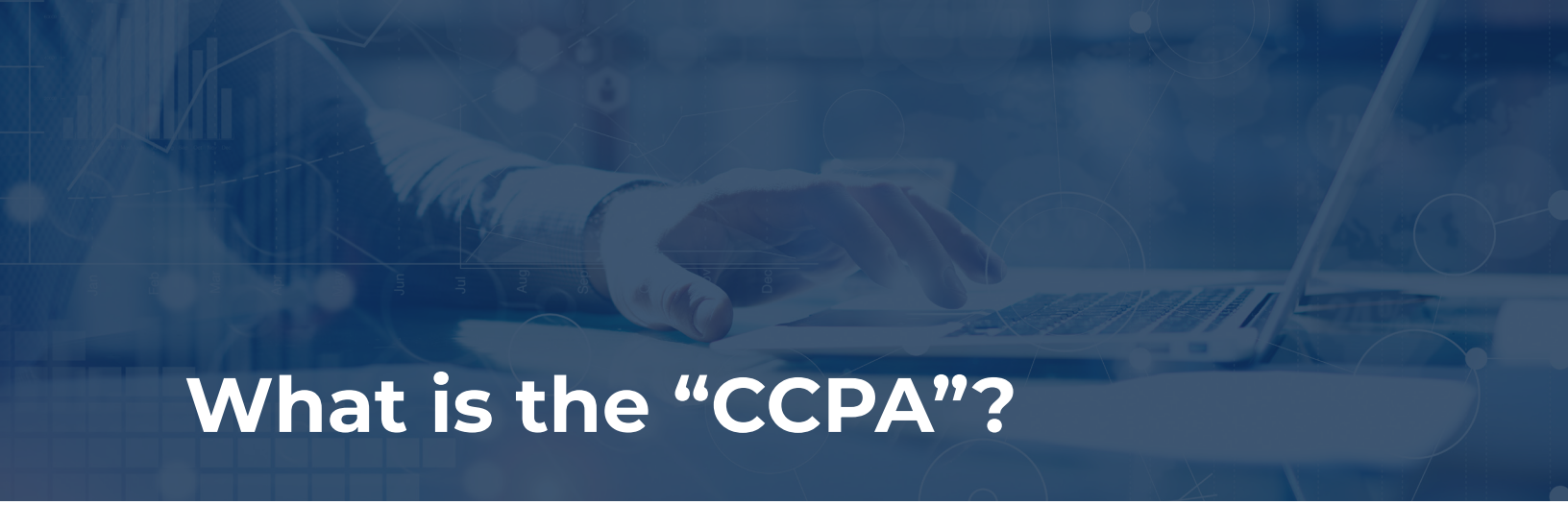
Is Your IR Website CCPA Compliant?

10 things you need to know about CCPA compliance

8/8/2019
IR Website CCPA Whitepaper
Tom Runzo, Equisolve
Sundeep Kapur, Paul Hastings LLP

EQUISOLVE



What is the “CCPA”?

The CCPA is the California Consumer Privacy Act (the “CCPA”), which passed on September 23, 2018, and goes into effect on January 1, 2020. However, personal information collected since January 1, 2019 is also within scope of the CCPA.

The CCPA governs how organizations collect, use, store, or otherwise process the personal information of “consumers,” regardless of the organization’s location.

The CCPA defines the term “consumer” as any California resident, including those that are B2B contacts, investors, or shareholders. We will use the term “consumer” and “California resident” interchangeably herein.

For example, if a company in Minnesota collects the personal information of California residents, the CCPA may apply to that company, even though it is located outside of California.

What does the CCPA have to do with my IR website?

As mentioned above, the CCPA governs how organizations use personal information of California residents, even if the organization itself is not located in California.

Since your IR website collects personal information from website visitors, shareholders, or investors in California, such as names, email addresses, job titles, IP addresses, cookie identifiers, search history, or log information, you may likely have to comply with the CCPA and its many obligations.

The California Attorney General can fine organizations $2,500 to $7,500 for violations of the CCPA

Further, California residents have a private right of action in the case of data breaches. In other words, California residents (and plaintiffs’ attorneys) can file civil lawsuits, including class

actions, for statutory damages between $100–$750 per consumer per incident or actual damages, whichever is higher. That means you may be liable for data breaches, even if there is no real harm. To make matters worse, California accounts for approximately 50% of all class actions lawsuits in the United States..

Who is responsible for CCPA compliance?

The CCPA applies to three types of entities: (1) "businesses," (2) "service providers," and (3) "third parties." Each term is defined within the CCPA and discussed below.

1. Businesses

Businesses have the vast majority of obligations under the CCPA.

A "business" is defined as any entity, wherever located, that does business in California, determines how consumers' personal information is used (i.e., to analogize to GDPR, acts as a "data controller"), and meets at least one of the following thresholds:

A. That has annual gross revenues of over twenty-five million dollars ($25,000,000).
B. Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in conjunction, the personal information of 50,000 or more consumers, households, or devices.
C. Derives 50 percent or more of its annual revenues from selling consumers' personal information.

You may think you don't "sell" any personal information.

However, "sell," "selling," "sale," or "sold" means 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 another business or a third party for monetary or other valuable consideration.
So, it's very broadly worded! For example, if your website uses retargeting or other advertising cookies or pixel tags on California consumers, this is likely considered a "sale" under the CCPA.

Finally, if you satisfy the above definition of "business," the entities that you control (or control you) are also considered businesses, provided that they share common branding with you (i.e., shared name, servicemark, or trademark).

2. Service Providers

The CCPA also applies to “service providers.” Put another way, even if you don’t fit the definition of “business,” the CCPA applies to you if you are a vendor that provides services to businesses.

A “service provider” is any entity, wherever located, that processes personal information on behalf of a business for a “business purpose.”

Like with the GDPR, a written contract must be entered into between businesses and service providers. This contract must expressly state that the service provider:

Processes the personal information for a “business purpose”;
Will not retain, use, or disclose the personal data for any purpose other than for the specific purpose of performing the services specified in the contract;
Will only use the personal information within the “direct business relationship” with the business;
Will not “sell” the personal data; and
“Certifies” that it understands its contractual restrictions and will comply with them.

So, whether you’re considered a “business” or “service provider” under the CCPA, you should make sure the data processing addendums you created for the GDPR are updated accordingly. If you weren’t subject to the GDPR, you should put together appropriate amendments in your Master Services Agreement or Terms of Service that account for the CCPA.

3. Third Party

A “third party” is any entity, wherever located, that is **not**:

A business that collects personal information from consumers;
A service provider; or
Any other recipient of personal information that has contractual restrictions similar to those between businesses and service providers.

The definition of “third party” is unclear in practice and adds more complexity to an already demanding statute.

However, a “third party” has a special restriction: it cannot “sell” personal information that was sold to it by a business unless the consumer has received an explicit notice and a chance to opt out of a sale (more on this below).

What do I need to do for my IR website to be CCPA compliant?

If you're a business, you have numerous obligations under the CCPA relating to your IR website. You have to:

1. Understand your data flows.

A core goal of the CCPA is to bring transparency to the consumer about the personal information collected and disclosed about her.

In order to comply with the CCPA, businesses need to know the sources from which they collected their personal information and to whom they disclosed that personal information, including to any vendors or other organizations.

2. Update your privacy policy.

The CCPA requires specific updates to your privacy policy. This includes:

A. The categories of personal information you have collected, sold, or otherwise disclosed about that consumer within the preceding 12 months;

B. The categories of sources from which the personal data is collected;

C. The business or commercial purpose for collecting or selling personal information;

D. The categories of third parties with whom the business shares personal information;

E. The specific pieces of personal information the business has collected about that consumer; and

F. A description of a consumer's right to access, delete, or opt out of the "sale" of that consumer's personal information (and how that consumer can request the business to carry out these rights); and

G. A description of any "financial incentive" programs.

As mentioned above, there is a 12-month "lookback" period for the CCPA. In other words, personal information you collected 12 months ago is still within scope of the CCPA.

Therefore, personal information you are collecting today should be contemplated when you're updating your privacy policy. This is because the CCPA goes into effect on January 1, 2020, and you have to disclose the personal information collected "within the preceding 12 months" (i.e., January 1, 2019).

3. Provide "access" rights to your personal information

Consumers can request access to the personal information you've collected, sold, or otherwise disclosed about them, pursuant to a "verifiable consumer request."

Generally speaking, you must provide similar information to what is disclosed in your privacy policy. However, there are two key differences.

First, where you have sold or disclosed personal information, you must provide two separate lists to the consumer requesting access:

A. The first list must contain (a) the categories of third parties that were sold personal information and (b) the categories of personal information sold to such third parties within the preceding 12 months.

B. The second list must contain (a) the categories of third parties that the business disclosed personal information to for a "business purpose" and (b) the categories of personal information disclosed to those third parties for a "business purpose" within the preceding 12 months.

Second, where a consumer requests the right of access, you must provide the specific pieces of personal information in a portable format and, to the extent technically feasible, in a "readily useable format" that allows the consumer to transmit this information to another entity without hindrance.

This is similar to the right of portability under the GDPR; businesses can consider providing the personal information in .csv or JSON or another format that may be considered "portable."

4. Provide “deletion” rights to a consumer’s personal information.

As with the GDPR, the CCPA provides a right for a consumer to delete any personal information about her pursuant to a “verifiable consumer request.”

Further, where a business receives a deletion request, it must direct its service providers to delete the personal information as well.

However, there are numerous exceptions to this deletion right, such as where personal information is necessary for debugging/security purposes, completing a transaction, complying with legal obligations, or “solely internal uses” that the consumer would expect from the business.

5. Ensure your website and back end systems are secure

The CCPA requires that businesses implement and maintain “reasonable security procedures and practices appropriate to the nature of the information.”

If a consumer’s non-redacted or non-encrypted personal information is subject to a breach, and the business did not have such reasonable procedures and practices, then a consumer may bring a private right of action (and, more concerningly, plaintiffs’ lawyers can bring class actions as well).

Businesses can start by implementing necessary security measures. Examples of not having “reasonable security procedures and practices” likely include a website without HTTPS (SSL), the lack of server logs, and unencrypted public networks (in use or at rest).

You should also be sure to document your security procedures and practices in case of an audit.

6. Set appropriate retention periods

The more data you hold, the more potential liability you have in case of a data breach. You should ensure that your personal information is subject to strict retention periods.

The days where U.S. companies held onto all data forever is slowly coming to an end, as states pass laws that impose more liability on companies for data breaches.

Be sure to understand what personal information is truly needed and start implementing documented retention schedules.

7. Put a "Do Not Sell My Personal Information" link on your homepage and your privacy policy.

If a business "sells" personal information, it must add a "clear and conspicuous" link titled "Do Not Sell My Personal Information" on its website's homepage and every page that it collects personal information on. It must also add the link, along with a description of the right, in its privacy policy.

Key details of this opt-out right include the following:

A. The "Do Not Sell My Personal Information" link must enable a consumer, or any other person authorized by the consumer, to opt out of the sale of that consumer's personal information.

B. Once a consumer opts out, you must wait 12 months before re-asking that consumer to opt back in. You can only re-sell that information once the consumer opts back in.

C. You cannot ask the consumer to create an account in order to exercise their opt-out right.

Businesses should start thinking about how to design their "Do Not Sell My Personal Information" pages so as to effectuate this opt-out right. Interestingly, unlike other CCPA rights, there is no requirement that a consumer's opt-out request be verifiable, so it is unclear what information you can or cannot request from consumers (or their authorized representatives) to confirm that it is indeed them.

8. Do not discriminate against consumers for exercising their rights.

You cannot discriminate against consumers for exercising their rights as described above. Examples of discrimination include the following:

A. Denying goods or services to the consumer.

B. Charging different prices or rates for goods or services, including through the use of discounts or other benefits, or imposing penalties.

C. Providing a different level or quality of goods or services to the consumer.

D. Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

However, you may charge a consumer a different price or rate or provide a different level or quality of goods or services, if that difference is reasonably related to the value provided to the consumer by the consumer's data.

Further, you can provide financial incentives for the collection, selling, or deletion of personal information, provided you disclose the material terms of the financial incentives in your privacy policy and obtain opt-in consent from the consumer.

9. Train your employees on CCPA obligations

Your employees should be trained on how to effectuate consumer rights under the CCPA to ensure compliance. Indeed, the CCPA requires that employees are trained on the opt-out right and how it works.

This is especially key for marketing departments, which may sell personal information depending on the providers they use. If they are not aware that a consumer has opted out, then this can be trouble for your compliance program.

10. Enter into written contracts with your service providers

Make sure you update your written agreements with your service providers, with all the express provisions discussed in the Service Provider section above.

Common Misconceptions

"I am GDPR compliant and so I don't have to do much to become CCPA compliant."

This is a very common misconception. While the CCPA has clearly taken inspiration from the GDPR, the CCPA has many unique and complex requirements which require its own compliance initiative. This is true even of requirements that may seem similar conceptually (e.g., right of access, privacy policy updates).

“The CCPA will be preempted by federal law so I don’t need to worry about it.”

You should not expect a federal law to save you. It is still very early in the process for a federal privacy bill. Further, while many proposals for a federal law have been introduced to Congress, there is much disagreement over what the scope of such law could be, especially with respect to federal preemption. In fact, the topic of federal preemption is avoided in most proposals.

“I am a B2B company and so CCPA does not apply to me.”

This is untrue—the CCPA protects the personal information of all “consumers.” However, “consumer” is defined as any California resident. This includes those that are B2B contacts, shareholders, and investors.

“My company is not in California, nor are any companies I use, and so I am not subject to CCPA.”

The CCPA is agnostic as to where companies are located, so long as they process personal information of California residents.

“My website is not TLS/SSL compliant but that doesn’t mean I’m not in compliance with CCPA.”

The CCPA does not mandate specific security controls. However, it requires “reasonable security procedures and practices.” TLS/SSL compliance is an industry standard, and it will be difficult to defend that you have “reasonable security procedures and practices” if you are not TLS/SSL compliant.

“Small businesses are exempt from the CCPA.”

This is untrue. If you are a business that sells or collects the personal information of consumers, households, or devices, you may be subject to the CCPA, even if you don’t generate large amounts of revenue. Further, if you are a service provider to these businesses, you are subject to the CCPA. Finally, even if you are neither of the above, you may still be considered a “third party” under the CCPA.

“Certain industries are completely exempt from CCPA, like financial services or healthcare.”

Untrue. Industries aren’t exempt from the CCPA—specific categories of data covered by certain laws are exempted (e.g., protected health information under HIPAA or nonpublic personal information under GLBA).

Conclusion

The CCPA is the most comprehensive U.S. state privacy law to date, and the time to act is now. While the CCPA was clearly inspired by the GDPR, the CCPA is a very different law with unique and complex requirements.

At some point, the California Attorney General is expected to release regulatory guidance to clarify certain distinct provisions. However, since this guidance is expected to only cover certain limited aspects of the CCPA, companies should take steps now to begin navigating its many nuanced obligations and to avoid costly class actions and enforcement actions. In addition, don’t forget the 12-month lookback—what you are doing today may come into play next year.

Tom Runzo, CEO
2455 E. Sunrise Blvd., Suite 1201
Fort Lauderdale, FL 33304
954-858-8550
tom@equisolve.com | equisolve.com

Sundeep Kapur
Paul Hastings LLP
875 15th Street, N.W.
Washington, DC 20005
+1.202.551.1944
skapur@paulhastings.com | www.paulhastings.com