View this email in your browser

What You Need to Know About the New California Privacy Law

18/07/2019

Just when you thought that the GDPR (the European privacy law that came into force in May, 2018) was the only wide-ranging privacy law you needed to be prepared for, a new challenging privacy law is set to go into force. The CCPA (the California Consumer Privacy Act), which in some ways is broader than the GDPR, comes into force on January 1, 2020. There are some actions that most companies will need to take to ensure compliance with the new California law, such as including a "Do Not Sell My Personal Information" link on its website, and being prepared to respond to more extensive disclosures pursuant to consumer requests.

As an increasing number of jurisdictions (both different countries and individual states of the United States) are enacting privacy laws, we suggest that our clients adopt a more strategic, worldwide approach to their data protection policies. Therefore, we encourage our clients to both make themselves familiar with the CCPA, as well as consider it in light of GDPR as well as other comparable requirements.

In a nutshell, what is the CCPA?

The California Consumer Privacy Act ("the CCPA") creates new obligations for companies that do business in California. Like the GDPR, the CCPA's goal is to give consumers an effective way to control their personal information and to increase the protection of their privacy rights. The exact enforcement date is

unclear, but enforcement actions may begin in July 2020 or even earlier.

To which companies does the CCPA apply?

The CCPA applies to companies that:

1. are for-profit businesses,
2. collect consumers' personal information (or on behalf of which such information is collected), and
3. do business in California (even remotely),

if they meet one or more of the following three criteria:

- Have annual gross revenues in excess of $25 million *(although the CCPA does not specify whether this is calculated on a worldwide basis, or just revenue generated from California, the consensus seems to be that this refers to the worldwide revenue)*; or
- Annually buy, receive, share and/or sell the personal information of at least 50,000 California consumers, households or devices; or
- Derive at least 50 percent of their annual revenue from selling California consumers' personal information.

The CCPA also applies to companies if they control or are controlled by an entity that meets one or more of the above criteria and shares common branding (such as the same trademark).

"*Doing business*" in California is not defined by the CCPA, but it will capture companies with links or ties to California. In order to ascertain whether a company *does business* in the State of California, companies should consider the following factors, which will probably be taken into account:

1. whether the company has a physical address or employees in California,
2. whether the company has any type of license or regulatory authorization to conduct business in California,
3. whether the company pays taxes in California,
4. whether the company sells into California or is involved in transactions for financial gain in California, and
5. whether the company monitors behavior of California residents, such as by creating profiles.

If a company does not meet the above criteria, could it still be affected by the CCPA?

Yes. Like the GDPR, the CCPA could also apply "indirectly", for example, through an agreement with a customer. Businesses that are subject to the law will likely want to ensure that their service providers protect information in a way that does not cause the business to violate the CCPA.

What are the consequences of violating the CCPA?

Among other consequences, a company found in violation of the CCPA could face:

1. a civil penalty of up to $2,500 per violation,
2. a civil penalty of up to $7,500 per intentional violation,
3. exposure to damages (in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater), and/or
4. injunctive or declaratory relief.

Currently, only the California Attorney General can bring a claim (except for data breaches, where the affected consumer can also bring a claim), but there have been amendments to the CCPA introduced in the California legislature which would expand the "private right of action". This would expose companies to a much wider litigation risk. Businesses have managed to defeat such proposals so far, but proponents have vowed to reintroduce such legislation in the future.

Is the CCPA similar to the GDPR?

Many of the concepts and obligations found in the CCPA are similar to those found in the GDPR, although they are not identical. Therefore, companies that underwent a robust GDPR-compliance exercise will be better prepared to comply with the CCPA but, unfortunately, will not be fully prepared.

What are the new rights that the CCPA gives to California consumers?

The CCPA gives California consumers the right to request that a business:

- disclose the categories and specific pieces of personal information it has collected
- disclose the categories of sources from which the personal information is collected
- disclose the business or commercial purpose for collecting or selling the personal information
- delete any personal information about the consumer that the business has collected from a consumer, subject to certain exceptions; and
- not "sell" the consumer's personal information (*Our comment: note that the concept of "selling" is defined extremely broadly*).

How does my company prepare for the CCPA? What are the main “action items”?

- Map out the personal information that relates to California residents (and do not forget to include cookies, analytic tools, trackers, inferences drawn from any personal information, profiles (e.g. preferences, characteristics, behavior or attitudes) and “Household” and “device” data)
- Implement a process for responding to access and deletion requests

- Implement a process for providing and honoring individuals' opt out requests
- Review third-party agreements
- Review security and incident response policies/procedures
- Train employees
- Update your privacy policy and California-specific privacy description (and ensure it is amended at least every 12 months), as required by the CCPA
- Implement two methods for consumers to send in requests to exercise their rights (including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address). (*Our comment: note that, as with a number of these provisions, there is legislation pending in the California legislature which may revise the obligation. In this case, there is legislation pending which will exempt the requirement for a toll-free number if the business operates exclusively online).*
- Implement a clear and conspicuous link called "Do Not Sell My Personal Information" on your homepage or consider creating a homepage that is dedicated to California consumers
- Assess your financial incentives/loyalty plans (if any)

When should companies start preparing for the CCPA?

Certain actions should definitely be completed by late 2019 (such as updating your website privacy notice or implementing the "Do Not Sell My Information" button). However, the CCPA includes some provisions requiring companies to respond to consumer requests about data collected or disclosed in the immediately preceding 12 months. Therefore, if, for example, a request is filed by a consumer in September 2020, the company may need to have access to that consumer's information dating back to September 2019. In order to be able to respond properly to such requests, companies should implement certain aspects of CCPA compliance as soon as possible.

How does CCPA compliance fit into our clients' worldwide data protection strategy?

The CCPA is just the latest jurisdiction to have a separate privacy law. Some other states (including Nevada, Maine and Vermont) have already enacted more narrowly tailored privacy laws. Many other states (including New York, Massachusetts, Pennsylvania, Texas, Washington State, Hawaii and Rhode Island) are considering such laws. We suggest that our clients consider adopting global data protection practices that are driven by the various local requirements.

Contact Information

David Mirchin,
Partner
dmirchin@meitar.com

Ignacio Gonzalez Royo,
Partner
ignaciog@meitar.com

Tali Yavin-Surasky,
Partner
taliy@meitar.com

For additional information about our firm's Technology group, click here

---