The California Consumer Privacy Act: Are You Ready?

By David R. Schwartz

The California Consumer Privacy Act ("CCPA") is a comprehensive new consumer data protection act set to take effect on January 1, 2020.

The law greatly expands consumers' rights and abilities to control the data which they submit to large companies, and creates numerous additional obligations for such companies with respect to tracking the consumer data they collect.

With the United States Congress still unable to enact a national data privacy statute, California is taking the lead and setting forth its own far-reaching new privacy law. For-profit companies which handle the personal information of California residents will need to comply with the new law; accordingly, Sacramento legislators have effectively instituted a de facto national standard.

With six months to go, here's a primer on the CCPA, and what you need to do to get your website ready for the New Year:

1. **Does the CCPA apply to my business?**

The CCPA applies to for-profit entities doing business in California that:

- Have gross annual revenues in excess of $25 million; or
- Possess (annually buys, receives for commercial purposes, sells or shares for commercial purposes) the personal information of 50,000 or more consumers, households, or devices; or
- Derive 50 percent or more of its annual revenue from selling consumer information.

The CCPA also applies to any entity that (1) controls or is controlled by a business that meets any of the above thresholds and (2) shares common branding with that business.

Note: it is currently unclear whether the $25 million threshold applies to a company's California revenue only, or to its overall revenue. This is an open issue that is likely to be resolved by amendment prior to January.

2. **How does the CCPA define "personal information"?**

The definition of "personal information" under the CCPA is extremely broad: "information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, *with a particular consumer or household*…" (emphasis added) such as identifiers (real name, alias, postal address, unique identifier, online identifier IP address, email address, account name, social security number, driver's license number, passport number), physical characteristics or description, insurance policy number, education, employment history, financial information, medical information, biometric information, and geolocation information.

It does not include publicly available information, which is information lawfully available from federal state or local government records.

Note that this new definition of personal information is the most expansive of any privacy law in the United States. It also differs from the European General Data Protection Regulation (GDPR) in that it extends to *households*, while GDPR limits consumer information as personal only. However, while referenced, the CCPA does not currently define the term "households".

Note also, that another open question is whether the CCPA applies to employee data. The CCPA defines a "consumer" as a natural person who is a California resident, but there is no requirement that such person have purchased goods or services in connection with data submission. Given that employment related information is considered personal information, employers who meet any of the above qualifying revenue or data collection thresholds should be prepared to comply, absent regulations or amendments in the coming months that specifically say otherwise.

3. **What new rights will California residents have under the CCPA?**

Most residents of the East Coast and Midwest look longingly towards California during long winter months. Now they will have another reason to envy residents of the Golden State. California residents will have the right to know the information large companies collect about them, the right to tell a business not to share or sell their information, and to seek legal redress if businesses don't keep their information safe. Here's what California residents will be able to request of businesses under the CCPA concerning their personal information:

(1) Right to Be Informed Prior to Collection: That a business disclose what categories of data will be collected prior to/at the point of collection, and to be informed of any changes to this collection;
(2) Know the Data Collected: That a business disclose the categories and specific pieces of information the business has collected about the consumer, twice per year, at no cost to the consumer;
(3) Know the Purpose Underlying the Collection: That a business disclose the business and commercial purposes for which the categories of personal information is collected and used;
(4) Right to Delete: That a business delete any personal information about a consumer which the business has collected (subject to certain exceptions, such as: completing a transaction, detecting security incidents, repairing errors, or exercising free speech or other rights);
(5) Know Third Party Categories: Disclose the categories of third parties with whom the business shared the consumer's information;
(6) Right to Opt-Out: Not sell the consumer's personal information.
(7) Right Not to Be Discriminated Against: A business cannot deny goods/services to a consumer who makes any of these requests about their personal information.

Businesses must provide easy accessible, free methods for consumers to request this information, and then typically respond to these requests within 45 days.

Note that businesses must also set forth a specific opt-in for the sale of personal information concerning children between the ages of 13 and 16. For minors under 13 years, parental or legal guardian consent must be obtained.

4. Does our Business Need to Update Our Website for the CCPA?

The short answer is: Most likely, yes!

The CCPA requires that companies which must comply under the law now must have an additional California privacy notice:

- A website must have a clear and conspicuous link to a "Do Not Sell My Personal Information" web-based opt-out tool.

Within the privacy policy, a business must:

- Proactively explain its data practices by listing the categories of personal information that the company has collected, disclosed, or sold within the previous year;
- Describe California residents' rights under the CCPA;
- Designate methods for submitting data access requests, including, at minimum, a toll-free telephone number and a website address (if applicable);
- Describe any financial incentives it gives to consumers for providing their data or not exercising their rights.

5. What Does Our Business Need to Do Beyond Updating Our Website?

Depending on your existing data policies and procedures, getting your information technology infrastructure to be in compliance with the CCPA may be quite time consuming.

High revenue businesses that collect personal information from California residents need to create and update their internal policies, systems, and methods so they are ready to comply with the CCPA come January 2020. To that end, companies should start planning now by:

- Obtain a toll-free telephone number that will be dedicated to handling consumer data access requests;
- Create a web page linked from the "Do Not Sell My Personal Information" enabling a user to opt-out of the sale of personal information.
- Implement processes to obtain parental or guardian consent for minors under 13 years of age and affirmative consent from children between the ages of 13 and 16 years of age for data sharing (i.e. establish clear procedures for such users to "opt-in" to data sales)
- Create a tracking system whereby if a California consumer opts-out of the sale of his/her personal information, that the business will not request that the consumer opt-in to such sale for at least 12 months from the date of the opt-out;
- Design a roadmap to easily track and report the destination(s) of all the data the business collects.
- Review vendor contracts concerning any vendors with access to consumer information to determine how such data is retained, secured, and disposed.

With an estimated 40 million residents, companies will need to be prepared if Californians start making requests concerning their data en masse.

6. What happens if our business does not comply?

Violations of the CCPA can become very expensive very quickly.

Businesses can be fined up to $2,500 for each violation and up to $7,500 for each intentional violation of the CCPA, enforced by the California Attorney General's office, if a violation is not cured in 30 days (note: the 30 day cure period may be revised in the coming months). Note that enforcement will be delayed until 6 months following publication of the Attorney General's implementation guidelines or July 1, 2020, whichever comes first.

Data breach incidents concerning California resident information which is "non-encrypted" or "non-redacted" are subject to additional civil penalties. A consumer may bring a legal action for damages ranging from $100-$750 per incident, or actual damages, whichever is greater. California residents have the right to enforce the CCPA via private action.

7. Are there exceptions to the CCPA?

Yes. If any of the obligations conflict with existing state or federal regulations, the CCPA provides for exceptions.

There are limited exceptions for certain types of personal information under the CCPA (not necessarily for businesses in such industries) already subject to state or federal regulation. Such categories include:

- Medical information / protected health information governed by the California Confidentiality of Medical Information Act or the privacy, security, and breach notification rules established by the federal Health Insurance Portability and Availability Act (HIPAA);
- Information provided to or from a consumer reporting agency limited by the federal Fair Credit Reporting Act;

- Financial information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act; and
- Personal information collected, processed, sold, or disclosed pursuant to the federal Driver's Privacy Protection Act.

There is also a specific exception for aggregated anonymized consumer information (for example, tracking the total number of visitors to your site).

There are numerous bills moving through the California legislature right now to provide additional exemptions. The coming months will likely bring additional modifications.

CONCLUSION

In the information age, information control, monitoring, access, storage, retention and disposal are of increasing importance. Every company needs to think of themselves as a repository of data. It is prudent to assess your organization's present data collection practices and internal capabilities to commence any and all changes needed to ensure a smooth transition to California's new privacy frontier.

For more information, please contact the author.

David R. Schwartz is a Partner at Raines Feldman LLP and heads the firm's Intellectual Property, Technology, and Privacy Practice.