# Privacy Alert: Are You Ready for the California Consumer Privacy Act (And the Lawsuits to Follow)?

October 14, 2019

The wait is finally over. On October 11, California Governor Gavin Newsom signed into law what is considered to be the toughest data privacy law in the United States. The groundbreaking California Consumer Privacy Act (CCPA), which becomes effective January 1, 2020, may require you and your service providers to add new policies, systems, and processes to comply with the new law.

How much do you know about the personal data you collect on your customers and employees? If you are a franchisor what access do you have to personal information collected by your franchisees? What security systems and processes do you use to protect against data breaches? If you do not know the answers to these questions you better pay closer attention to data security, what personal data you collect, and how it is used in your business.

You probably just became used to the European data privacy law known as the General Data Protection Regulation (GDPR) and thought your data privacy concerns were limited to European customers. Sorry, but enhanced data privacy rights have crossed the pond and are now extended to California residents.

The GDPR and CCPA do not care where your corporate office is located. They apply to and cover the individual, and are based on the residence of the individual whose personal data is collected. Even employees and households are covered under the CCPA.

Failure to comply with the new CCPA could expose your business to significant monetary damages. No longer are your risks limited to a potential enforcement action by a state attorney general's office, the Federal Trade Commission (FTC), or other government regulator. Such government actions were rare and mainly focused on companies like Facebook and Google. Now you can face a multimillion-dollar class action lawsuit based upon the first of its kind CCPA private right of action. Plaintiffs' lawyers are ready and willing to bring CCPA actions against any and all businesses who fail to implement reasonable data security and suffer a data breach.

**Does the CCPA Apply to Your Business?**

The CCPA applies to any business (nonprofits excluded) that collects personal information from California residents and has at least one of the following:

- Annual gross revenues of $25 million or more.
- Buys, receives, sells, or shares the personal information of at least 50,000 California residents, households, or devices annually.
- Derives a minimum of 50 percent of its annual revenue from selling California residents' personal information.

Note that definition of the term "consumer" in the CCPA is broad and includes "households" and employees.

**New Private Right of Action**

While much attention has been given the new rights afforded California consumers to have more access and control over use of their personal data, the greatest risk to a business is the new private right of action — with substantial statutory damages — for data breaches. Consumers can now sue a company when their "non-encrypted or non-redacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the **duty to implement and maintain reasonable security procedures** and practices appropriate to the nature of the information."

Plaintiffs' lawyers and their consumer clients who are the victims of a data breach can now seek statutory damages of between $100 and $750 per consumer per incident, actual damages, and injunctive relief. There is no need to demonstrate actual harm to the consumer.

If a large number of records holding personal information is breached, the potential financial exposure will be enormous. For example, a breach involving 50,000 residents could result in a $37.5 million claim.

The CCPA private right of action is limited (as of now) to data breaches. Any other noncompliance with the CCPA may however subject a business to enforcement actions by the California Attorney General with civil penalties of up to $7,500 per violation.

## What Should You Do to Get Ready?

### Data Mapping

Under the CCPA, consumers will have the right to request that you disclose what personal information you collect and for what purposes, and (with some exceptions) request that you delete any such personal information.

Perform data mapping as necessary to inventory the personal information collected on California residents, households, and devices. For what purposes is such data collected, who is it shared with, and where is it stored. Now is a great opportunity to minimize the personal data you collect. You cannot lose what you do not have.

### Evaluate Business Processes

New business processes and system changes may be necessary to respond to and handle data access and deletion requests from California residents as well as any requests to opt out of data sales. You must be prepared to disclose and deliver the required information to a consumer making such request free of charge within 45 days of receiving a verifiable request. The proposed regulations issued by the California Attorney General offer some guidance on how to respond to and verify such consumer requests.

### Update Privacy Policies

Privacy policies and notices may need updates with new disclosures regarding consumer rights to data access and deletion. Consumers must be notified of and be able to opt out of the sale of their personal information, including use of a DO NOT SELL choice on your website. Privacy notices must indicate the categories of personal information collected and the purposes for which they are used. If you do not sell personal data you should include an affirmative statement that you have not sold information to third parties in the preceding 12 months. If your privacy policy does not already include such disclosures now is a good time for an update.

### Data Security

If nothing else, the CCPA private right of action should elevate security as a major concern. Consumers can now sue a company when a business has failed to implement and maintain reasonable security procedures and practices.

Several years ago the California Attorney General's office identified the Center for Internet Security (CIS) controls as one example of a data security standard that is "reasonable." Core components of the CIS controls include a written information security program, oversight by a designated security officer or

supervisor, employee training, vendor management, an incident response plan, and ongoing risk assessment and management . A data breach due to the failure to implement CIS controls might be viewed as "unreasonable" under the CCPA standard. Check with your IT group or engage a consultant to make sure you have " reasonable " security procedures in place.

The creation of written information security programs and incident response plans and teams, as necessary to handle unauthorized access and potential data breach notification requirements, are now more critical than ever before.

**Vendor Management**

Review contracts with vendors who process or handle customer data or personal information to assure they are complying with the CCPA and other data privacy laws, and — if necessary — provide an addendum to cover CCPA compliance.

**Consider Cyber Insurance**

It may be worth purchasing insurance now before CCPA lawsuits drive up costs.

**Monitor Legal Developments**

On October 10 the California Attorney General issued proposed regulations on how CCPA will be implemented. These are draft regulations with public hearings scheduled in early December and written comments accepted until **December 6**. Once finalized these rules will govern compliance with the CCPA. The draft regulations detail what notice must be provided at time of data collection, information required in privacy policies, business practices for handling consumer requests for access or deletion of data, verification procedures, training and recordkeeping, and special rules for the collection of information from children.

**CCPA enforcement will commence six months after the Attorney General regulations are finalized or July 1, 2020, whichever occurs first.**

CCPA has motivated other states to introduce copycat legislation. In the absence of federal privacy legislation other states, including New York, Massachusetts, Nevada, and Washington have passed or introduced new data privacy laws similar to the CCPA. It's likely that even more states will enact such CCPA type laws.

Finally, Alastair Mactaggart, the California real estate mogul whose ballot initiative led to enactment of the CCPA, has announced a new ballot initiative for November 2020 that among other things would cover the collection of health and financial data and impose penalties for the sharing and selling of data about children. Stay tuned.

Gray Plant Mooty will be holding webinars on the CCPA and how to operationalize the various legal requirements. If you are interested in more information on these webinars or have any questions regarding CCPA compliance, please contact Michael Cohen (612.632.3345).

*The content is intended for informational purposes and is not legal advice or a legal opinion of Gray Plant Mooty.*