FLASTER GREENBERG
Attorneys at Law | A Professional Corporation

Enforcement of the California Consumer Privacy Act Begins July 1, 2020: Quick Compliance Tips

FG Law Blog

June 19, 2020

Krishna Jani

The California Consumer Privacy Act ("CCPA") is one of the strongest and most comprehensive consumer data privacy laws in the country. It is designed to protect the data privacy rights of citizens living in California, and can thus impact any business that has customers in California. In essence, the law requires that companies provide more transparency to consumers about what companies are doing with their data.

California Governor, Jerry Brown, signed the CCPA into law in June 2018. The law went into effect on January 1, 2020. Enforcement of the CCPA begins July 1, 2020 despite the fact that regulations surrounding the law have not yet been finalized. Moreover, California Attorney General ("AG"), Xavier Becerra, has confirmed that enforcement will not be delayed due to the COVID-19 pandemic. Accordingly, companies should not wait for the final regulations to establish CCPA compliance plans.

Which Businesses Does the CCPA Affect?

Businesses subject to the CCPA generally fall into one of three categories:

- Businesses that earn at least $25 M in annual revenue
- Businesses that receive, buy, or sell personal data of 50,000 or more consumers or devices
- Businesses that earn more than 50% of their revenue from selling data

Which Businesses are Exempt from the CCPA?

Businesses that are exempt from the CCPA include:

- Health providers and insurers already subject to HIPAA laws
- Financial companies covered by the Gramm-Leach-Bliley Act
- Credit reporting agencies under the Fair Credit Reporting Act

What Rights do Consumers Have?

The CCPA grants consumers more control over the sharing of their data by, for example, providing "opt-out" provisions to prevent their information from being used in a way they do not want or, conversely, "opt-in" consent clauses for minors under 16—meaning the child (or parent or guardian if the child is under 13) must affirmatively authorize the sale of their personal information.

If consumers refuse to consent to the collection, storage, and sale of their personal data, or "opt-out," consumers have additional rights such as the right to request access for their personal information to find out in more detail about the specific pieces of information held by the business and the third parties that received their information. Moreover, if consumers exercise any of their rights, companies cannot then discriminate against them by denying them goods or services. Under this new law, consumers also have the right to have their information deleted (with some exceptions).

What will Enforcement of the CCPA Look Like?

The AG is tasked with enforcing the CCPA, and the CCPA also provides for a private right of action in instances where there is a theft or disclosure of non-encrypted or non-redacted information. The statutory damages for these types of violations range from $100 to $750 per violation, or actual damages, whichever is greater.

It is important to know that there is no requirement that consumers *prove* that they incurred an actual financial loss to recover statutory damages under the CCPA. They only have to show that the company violated the law. For this reason, companies should be cognizant of the risk of class-action lawsuits.

Quick Compliance Tips

- Lay the foundation for compliance: identify and demarcate your data assets so that you know where personal information is being stored, and whether the data is at risk by determining who has access to it.
- Implement cleaner security protocols: limiting data access to those who need it can be an effective way to increase data security. You may also want to consider archiving or deleting stale personal data to mitigate unnecessary risk.
- Stay on alert: new cybersecurity and data privacy threats emerge every day. Making sure that you and your team adjust privacy and security settings as needed and continue to evaluate your existing systems is crucial for long-term compliance.

Takeaways

Since the U.S. does not have a comprehensive federal data privacy law, companies should play it safe and align their data security and privacy practices with the CCPA whether they are specifically subject to the law or not. More and more states are enacting data privacy laws that closely follow the structure and requirements of the CCPA, including New York, Massachusetts, and Maryland, and there are signs that more states may follow suit.

It's best to have your privacy policy reviewed by a professional in order to stay in front of these types of consumer privacy laws.

In an effort to help clients avoid unwanted penalties, Flaster Greenberg attorneys can review privacy policies for CCPA compliance. Please contact Krishna Jani or Donna Urban of Flaster Greenberg's Privacy & Data Security Group to ensure your business is up-to-date with the current privacy laws or if you are unsure whether your business is exempt from CCPA.