Subscribe To Data Privacy Law

Email Address *

SUBSCRIBE!

Search Posts

Categories

- Webinars & Podcasts
- Jaffe Updates
- News
- Electronic Payments Law +
- Michigan Green Law +
- Data Privacy Law +
- Immigration Law +

Download PDF

DECEMBER 6, 2018 | JAFFE LAW

Executive Summary: The California Consumer Protection Act: Who Does It Affect and How?

With concerns about privacy and data security at an all-time high, California is leading the way in consumer protection and access of one's own personal information. Passed in 2018, the California Consumer Protection Act (CCPA) is set to take effect on July 1, 2020. The goal of the CCPA is to provide consumers with more transparency about the information gathered from them and power over what happens to that information. From an article by Daniel Ungar in the Michigan IT Lawyer, the law provides the following five rights:

1. The right of Californians to know what personal information is being collected about them.
2. The right of Californians to know whether their personal information is sold or disclosed and to whom.
3. The right of Californians to say no to the sale of personal information.
4. The right of Californians to access their personal information.
5. The right of Californians to equal service and price, even if they exercise their privacy rights.

Who is Protected and Who Must

The CCPA defines a protected consumer as a natural person who is a California "resident," defined under Section 17014 of Title 18 of the California Code of Regulations as an "individual who is in the State for other than a temporary or transitory purpose and . . . every individual who is domiciled in the State who is out of the State for a temporary or transitory purpose."

A business required to comply with the CCPA is a legal entity that: (1) has an annual gross revenue greater than $25,000,000.00; (2) buys, sells, or shares/receives for commercial purposes, the personal information of 50,000 or more consumers, households, or devices; or (3) derives 50% or more of its annual revenue from selling consumer personal information.

Confusion as to what entities fall under these three categories has already surfaced. The CCPA does not indicate whether the metrics used to determine whether a business must comply are calculated solely using a company's business in California or the aggregate of the company's business inside and outside of California. This ambiguity leaves a large number of businesses unsure as to whether they are required to comply with the CCPA.

What Effect Does this Have on Businesses?

On the federal level, personal data is protected through a sector-based approach, meaning the type or source of information determines the applicable laws (e.g. HIPPA, GLBA, FERPA). The CCPA attempts to create an omnibus approach, much like the EU's approach under the General Data Protection Regulation (GDPR), providing blanket protection for citizen information regardless of the source or content.

Most individuals agree that protecting personal information needs to be a priority; however, the downstream effects of data protection laws must be quantified. In order to comply with the CCPA businesses must know exactly what personal information they have collected and be able to easily access the data if a consumer requests information collected about him/herself. The most efficient way for a business to organize the data it collects is to keep it in one location; however, people have raised concerns that this pooling of data may increase the risk of unauthorized access and breaches.

Additionally, if an individual requests their personal information subject to the CCPA, the business must be able to confirm that person's identity. This will require the business to collect more information about the individual. Further, if the person inquiring about their information

asks for the information to be deleted, the business must keep record of the deletion and, most likely, what was deleted. As a result, there are concerns that this just creates a vicious cycle of collection for the sake of deletion, defeating the purpose of deletion itself.

The issues discussed preceding paragraphs require forward-thinking from businesses. There is a strong need to create strategic plans for how to adequately secure an individual's data and how to comply with the requests of individuals. Neither of those tasks comes without a price tag. The financial stress the CCPA will impose on businesses is hard to determine at this point. Companies like Google and Microsoft will have no issue finding their efforts to comply with the CCPA, but businesses with less disposable income will need to develop creative solutions for compliance.

Conclusion

While many businesses do not fall within one of the three categories for compliance with the CCPA, that does not mean those businesses should not take note of the law and take steps to prepare themselves for compliance with similar laws in the future. The trend of strong protection paired with open transparency is likely to drive the world of data in the future. California is not the only state strengthening its data protection laws and the United States is not the only country tackling this issue. As a result, businesses that collect or use personal information of individuals must be aware of changes in data protection laws throughout the country and world.