Another Win for Global Consumer Data Rights

California Data Privacy Law

The California Consumer Privacy Act (CCPA) of 2018 continues a growing global crusade for increased consumer privacy rights and data discretion in the wake of the EU General Data Protection Regulation (GDPR), and it will have a number of similar implications on organizations conducting business in California, USA.

Starting in 2020, the law requires organizations to disclose what consumer information is collected from California residents and how it will be used. Any organization that does business in California with more than US $25 million in annual gross revenues will be required to adhere to stricter online privacy laws and firmer ground when it comes to how the data of California residents are collected, controlled, secured and used. CCPA ultimately helps consumers better understand corporate data collection policies and empowers them to act in their own best interests.

Similar to the EU’s GDPR mandate that took effect in May 2018, CCPA expands personal data protections for today’s increasingly connected world, including the right to be forgotten, a right to portability and a right to access data. But there are some nuanced differences in the language of these rules and how each is governed and enforced.

One thing is clear when it comes to CCPA and GDPR: The scope and definitions of “data” and “personal information” are incredibly broad. Even these two very similar laws address different aspects of those terms and, perhaps, further cloud any comprehensive meaning of the terms in context of today’s digital business landscape.

Even so, GDPR laid the foundation for new regulations such as CCPA, setting in motion a snowballing global movement that checks the power of organizations when it comes to data collection and processing and strives to restore data control to its rightful owners.

About CCPA

CCPA was backed with bipartisan support in the California Legislature on 28 June 2018 and approved on 2 July 2018 by California Governor Jerry Brown. California state officials made such quick work of the data discretion bill in part to keep another more restrictive privacy initiative off California’s midterm election ballot in November 2018.

That ballot measure, while similar in the oversight of consumer data protections, would have made it easier for individuals to sue organizations in breach and required a 70 percent supermajority in both legislative houses to amend the law going forward. Instead, legislators pushed CCPA through just a week after the proposal was introduced and hours before the deadline to pull the November ballot initiative.

About Dave Brunswick

Dave Brunswick has more than 25 years of experience in technical sales, presales, technology strategy, engineering, product management and product development, including holding senior consulting and architecture roles throughout the managed file transfer software market. He currently serves as vice president of North America presales and solution support for Cleo.
While some privacy advocates feel CCPA did not go as far as the ballot initiative in providing legal recourse for individuals whose privacy rights had been violated, many feel it is a step in the right direction in a country that has little in the way of privacy laws and is "a huge win and gives consumer privacy advocates a blueprint for success."2

The New Data Norm

For decades, organizations have used consumers’ personal information for their own benefit with little oversight on how those data are obtained, accessed and used. Mandates such as GDPR and CCPA are designed to encourage not only expanded data care and privacy, but also enhanced business transparency.

It is almost fitting, then, that just as organizations hit their stride with GDPR compliance, another data protection regulation comes along that helps establish further ground rules and necessitates additional action. The good news is, organizations that are already GDPR-compliant will have an easier time adhering to CCPA’s requirements.3

GDPR raised the bar on data privacy standards, increasing emphasis on respecting individual rights by giving back control of personal and sensitive information and mandating heavy financial penalties for organizations that fail to do so. CCPA similarly gives Californians unprecedented access to their data, and they will soon have the right to:

- Understand what personal information is being collected about them
- View and act on the personal information collected
- Know whether that information will be sold and to whom
- Deny the sale or disclosure of their personal information
- Request that organizations delete information they have collected

CCPA requires organizations to not only disclose what type of data they collect—including home addresses; employment information; Social Security numbers; email addresses; IP addresses; and such demographic information as gender, race and ethnicity—but also data about the data (i.e., metadata). This includes categories of personal data (“unique personal identifiers” as well as genetic and biometric data), categories of sources of data, and categories of third parties with whom the data are being sold or shared.

This requirement to disclose categories is notable as it aims to make organizations more selective about the data they collect rather than casting the widest net possible.4 Additionally, organizations will have to report how they use all these data for targeted advertising online.

"BOTH LAWS PROTECT AGAINST MAKING INFERENCESED AND BUILDING A “PROFILE” OF AN INDIVIDUAL BASED ON THE COLLECTED INFORMATION."

While many of CCPA’s ideas are similar to GDPR, culling some of the main points of each mandate can provide a better understanding of the hot-button issues regarding data privacy, how organizations are evolving their data collection and processing methods, and where data discretion laws are headed.

The following are some of the language and regulatory nuances concerning the principal concepts in CCPA and GDPR.

Who It Affects

The protected entity in CCPA is the “consumer” and his or her “personal information,” while GDPR focuses on the rights of “data subjects” and their “personal data.” While CCPA defines a “consumer” to be a natural person who is a California resident, the term implies a distinction between a person and a person who is purchasing goods and services.
CCPA also focuses on any personally identifiable information that, according to the legislation text, “could reasonably be linked, directly or indirectly, with a particular consumer or household,” which is implied in GDPR, but not explicitly stated. Both laws protect against making inferences and building a “profile” of an individual based on the collected information.

Who Must Comply
The CCPA is aimed at enterprises, while GDPR is geared toward data controllers and data processors. Both terms generally mean for-profit companies or organizations, with GDPR making a distinction between those collecting personal data and those using it. CCPA generally affects any organization that collects or sells California consumers’ personal information, which is much like GDPR in that an organization’s physical location is of little importance, applying to any organization inside or outside the EU that processes personal data of EU residents.

However, the CCPA’s language limits the impact to small businesses and extends to include organizations that explicitly aggregate and profit from selling consumer data. California’s law is applied to any organization that:

- Has an annual gross revenue of more than US $25 million
- On an annual basis, buys, sells, receives or shares (for commercial purposes) the personal information of 50,000 or more consumers, devices or households
- Derives 50 percent or more of its annual revenue from selling consumers’ personal information

Consent, Opt-In
Whereas GDPR requires organizations to obtain “freely given, specific, informed and unambiguous” consent before collecting any personal data, CCPA does not explicitly require organizations to gain consumer consent upfront to collect and process their information. However, CCPA does require opt-in before selling the information of anyone younger than 16 and consent of a parent or guardian for those under age 13. GDPR requires parental consent for those younger than 16.

ACCORDING TO THE CALIFORNIA LAW, AN ORGANIZATION WILL BE IN VIOLATION IF IT FAILS TO RESOLVE AN ALLEGED INCIDENT WITHIN 30 DAYS OF NOTIFICATION.

CCPA does allow consumers to opt out of their data being sold via “a clear and conspicuous link on the business’ Internet homepage, titled ‘Do Not Sell My Personal Information.’”

Disclosures
Both laws require disclosure when it comes to the types of data collected, though the scope of GDPR disclosures extends beyond those mandated by the CCPA. GDPR requires data subjects be provided an explanation that clearly states how the data will be used, the data’s retention period and other information. CCPA usually only requires disclosures for the previous 12 months of data collection and processing, whereas GDPR has no such limitation.

Perhaps most notable is that while GDPR and CCPA each require the disclosure of the individual rights as they pertain to data collection and processing, the rights are not identical. Consequently, enterprise privacy policies rewritten specifically for GDPR may not necessarily meet the CCPA’s requirements and likely will need to be updated.

Penalties
GDPR’s fine structure for a compliance failure is more severe overall—4 percent of the organization’s global revenue or €20 million (approximately US $23 million), whichever is greater. Organizations that violate any aspect of the CCPA face fines in the thousands of US dollars, ranging from US $2,500 to US $7,500 per infraction, depending on the context. However, CCPA allows compensatory recourse for consumers, with damages ranging from US $100 to US $750 per incident, though it is unclear just how much litigation will be allowed in pursuit of those awards.

According to the California law, an organization will be in violation if it fails to resolve an alleged incident within 30 days of notification. Organizations will
have 45 days to respond to consumer requests. Under GDPR, however, organizations have just 72 hours to report data breaches and violations to regulators.

**Conclusion**

The overarching theme regarding data privacy mandates such as GDPR and CCPA is that governments and regulatory agencies, in an increasingly digital world, recognize the growing need for expanded data security, data privacy and corporate transparency. Such measures are important steps in holding businesses accountable for how personal information is collected and processed, which has been surreptitious practice for too long.

While the main tenets of California’s data privacy law overlap with GDPR’s, CCPA seems to expand the definition of personal information in its inclusion of more specific data elements and the disclosure requirements for metadata surrounding aggregation and processing. The law certainly demonstrates forward progress on an evolving subject in the ever-evolving digital business domain.

Finally, the CCPA is just the first US domino to fall in the wake of the EU’s sweeping GDPR measure. California is the fifth-largest economy in the world, and CCPA will almost certainly open the door for other states (and countries)’ own data discretion standards. The comprehensive result of these efforts will further advance consumer data protections and enable individuals to regain control over how their personal data is collected and used.

**Endnotes**


6 Ibid.