Legal Insights

Wolters Kluwer

September 20, 2018

California v. GDPR: Compare and Contrast

By Cynthia J. Cole and Neil Coulson, Baker Botts LLP*

This is part of a continuing series of articles by Cynthia J. Cole and Neil Coulson on the legal developments and implications of changing U.S. data privacy laws and the General Data Protection regulation on U.S. companies. Here we compare the California Consumer Privacy Act of 2018 to the GDPR.

This document does not attempt to describe the full scope of the GDPR or U.S. data privacy laws or how companies can comply with the numerous requirements of either. This document is not intended to constitute legal advice and should not be relied on as such.

Introduction

Hailed by some as the GDPR 2.0, the California Consumer Privacy Act of 2018 ("CCPA"), passed after only a few weeks of deliberation, is a far cry from the sweeping legislation of the European Union. While it may be the toughest data privacy law in the United States, the law as it stands has much room for revision and extension before it comes into force on January 1, 2020. Unlike the GDPR, which focuses not only on the rights of individuals but also provides rules for companies to properly manage and process personally identifiable information ("PII"), the CCPA primarily provides a means for consumers to become informed about what PII has been collected by companies, which companies have that PII, and how that PII is used. While the CCPA does contain provisions which purport to allow consumers to demand the deletion of their PII, those provisions, as will be explored, are not nearly strong enough to give adequate protection nor are the CCPA's enforcement mechanisms up to the task before them.

Definitions (GDPR Article 4; CCPA 1798.140)

Defining the terms of a data privacy law is vital to determining both the scope of their protections as well as the burden of their implementation. Two key definitions arise in any discussion of data privacy: (1) to whom does the law apply, and (2) what information is covered.

Businesses

On its face, the CCPA only applies to certain businesses, namely a business which meet one of three thresholds: (1) has annual gross revenues of $25,000,000 or more; (2) buys, receives, sells or shares (for commercial purposes) the personal information of 50,000 or more consumers (located in the

* Baker Botts partner **Neil Coulson** is the Department Chair - Intellectual Property in London and Moscow. **Cynthia J. Cole,** CIPP/E, is Special Counsel in Palo Alto in Baker Botts' corporate, technology and privacy practice groups.

state of California); or (3) derives 50% or more of its annual revenues from selling consumers' personal information. On its face, the CCPA seems to apply only to relatively large businesses; however in the reality of the Internet age, it is incredibly easy for any company with a publicly accessible website to reach more than 50,000 people in California.

On the other hand, the GDPR applies broadly to any enterprise which either collects, controls, or processes information. There is no size or threshold requirements under the GDPR; any processing or collection of personal data must comply with the provisions of the GDPR.

Personal Data

Under both the CCPA and the GDPR, personal data is any data or information which can be used to identify, relates to, or can be associated with, a particular individual. This includes (but is not limited to): real name, aliases, postal address, email addresses, biometric information, and location data. The CCPA goes slightly further than the GDPR and includes information that can identify households as personal data as well.

Interestingly, both laws only protect personal data for natural living persons. Legal persons (corporations, etc.), while they obviously must comply with the provisions of both laws, do not obtain the same level of protection.

Consumer Rights

Both the GDPR and CCPA guarantee certain individual rights with respect to their PII, including a right of access, to be forgotten, and objection. At the same time, though, both laws contain rights which are not present in the other: the GDPR contains a right to data portability not present in the CCPA, while the CCPA contains a right to non-discrimination.

The Right of Access (GDPR Article 15; CCPA 1798.100)

Under both the GDPR and the CCPA individuals have the right to access PII collected (and sold) by a business. Under the CCPA this right includes information regarding the purpose of the collection, the categories of information collected, the categories of sources of the information, the categories of third parties with whom the data is shared, and specific PII that has been collected. While businesses need not proactively provide this information to every consumer, this information must be available upon request and delivered within 45 days, though an additional 45 days may be allowed if notice is given to the consumer.

The Right to be Forgotten (GDPR Article 17; CCPA 1798.105)

Also known as the Right to Deletion, this right allows for individuals to request deletion of any PII that the business has collected. Under the CCPA, though, there are a number of broad exceptions which allow a business not to comply with a deletion request. These exceptions include:

(1) compliance with another legal obligation; (2) use in purely internal uses; and (3) providing a good or service "reasonably anticipated" within the context of the relationship between the business and the consumer. Taken together, these exceptions allow significant opportunity for a business to keep PII even after a deletion request. For example, the legal obligation exception seems to allow for contractual obligations to overcome deletion requests.

While businesses must delete any PII they have collected, and inform third parties of the requirement, businesses needn't ensure, nor are they liable for, any third parties who fail to delete the information, requiring instead a consumer to then pursue those third parties themselves if they want PII deleted. This creates a greater burden on consumers who wish their information deleted, since they need now communicate and pursue all third parties that have received PII.

The Right to Object (GDPR Article 21; CCPA 1798.120)

Referred to in the CCPA as the right to "opt out," this provision allows for consumers to object to the sale of their information. Under the GDPR, this is actually a much broader right, allowing for data subjects to object to any use ("processing") of their personal information. Under the CCPA, the right to object is limited to objecting to sale of the information to third parties, leaving businesses, generally, free to put the data to whatever use they wish, without consumers being able to stop it. As discussed previously, a consumer could request deletion of information but with the broad exceptions available this would likely give a consumer little control over the use of information by a business.

The Right to Non-Discrimination (CCPA 1798.125)

This right, not present in the GDPR, guarantees that consumers cannot be denied service, charged different prices, or given a different quality of good or service because they have exercised any of their rights. While this seems like an important (and powerful) provision, it is actually incredibly problematic, because within the same section the CCPA allows for discrimination if the difference is "reasonably related" to the value of the consumer's data. In addition, this provision allows for the offering of "incentives" for allowing collection and sale of PII.

Under the current CCPA practical effect of this provision is unclear. Guidance on how to "value" a consumer's data is needed in order for businesses to properly tailor their policies in order to be compliant. The California legislature will also need to draw a clearer line between a program that is discriminatory as compared to a program that merely presents an "incentive" for a consumer to consent to sale and collection of information.

The Right to Notification (GDPR Article 14)

While similar to the right of access, above, this "right" places an affirmative duty on data controllers to inform data subjects when the subject's personal data has been acquired from a source other than the data subject. Although fairly broad and open ended, it requires businesses to make reasonable efforts to find and inform all data subjects whose personal data they have received.

Although the CCPA does require businesses, upon request, to divulge the categories of third parties with which they share information (CCPA 1798.110), there is no affirmative duty placed on businesses to inform consumers that their PII has been acquired.

The Right to Data Portability (GDPR Article 20)

This right, not present in the CCPA, allows for individuals to receive all PII they have provided to a controller in a machine-readable format. Individuals also have the right to transmit this information to another controller "without hindrance" from the original controller. This right is only available where the data processing is based on either consent or a contract between the parties, and the processing is carried out by automated means. While these narrow grounds might limit the usefulness of the right, its availability is still more useful than the silence of the CCPA.

One of the key advantages of this right is its ability to help encourage competition (or at the very least not stifle competition), since it allows for the easy transfer of already collected information, meaning that a new business need not, necessarily, have to collect information that is already available, so long as the consumer requests transfer of that information. Without it, businesses must each individually collect PII, which also increases the risk of a data breach and dissemination of PII, against the wishes of the consumer.

Processing

As mentioned above, the CCPA's primary focus is not on data *use* but on data *transparency*, so rather than defining proper methods and purposes to which PII can be put, the CCPA focuses instead on defining ways by which consumers can remain informed regarding which businesses have their information, what information those businesses have, and to what uses those businesses have put their PII (with little recourse for controlling those uses).

Lawfulness (GDPR Article 6)

Unlike the GDPR, which goes into significant detail regarding the "lawfulness of processing" and outlines circumstances under which a business may process information, the CCPA focuses more on transparency and sale. While allowing for consumers to see what information is collected (and with whom it is shared) and to restrict sale of PII, there is little that consumers can do to restrict or control what information is collected as well as what uses to which that information is put. As a result, while consumers may be able to see what PII a business has collected, there is little that they can do to restrict what a business "does" with that information (beyond restricting sale).

As discussed above, even the right to object to sale of their PII is a limited right, meaning that the practical effect of the CCPA is, primarily, to allow consumers to see what information is collected without having much recourse to control this data once it is collected. The GDPR, on the other hand, focuses more on ensuring proper "data stewardship," that is, ensuring that

companies who collect data use that data responsibly, in ways that are acceptable to consumers. This helps shift the burden of protecting PII from consumers, who are rarely capable of or interested in monitoring all uses of their data, to the businesses who rely on that data to remain profitable.

Security (GDPR Article 32)

Once data has been lawfully collected for a legitimate purpose, the GDPR still imposes certain security requirements that are intended to reduce the risk of a data breach and ensure that a minimum level of data security is maintained throughout processing. While the extent of this security will depend on a variety of factors, including the sensitivity of the data collected, the nature of the processing, and the cost of implementation, it still helps to guarantee that data controllers and processors will take appropriate care of data once it is collected.

No such requirement is found in the CCPA. Likely, the drafters of the CCPA rely on its enforcement mechanisms to encourage business to implement safety measures, without creating a cause of action for inadequate safety measures in the first place. This approach is problematic because, rather than ensuring a certain level of data security as an end itself, the CCPA treats an actual data breach as the only time that a business can be held liable for failing in its duties. Such an *ex post* enforcement mechanism could cause an increase in the risk of data breaches,[1] since, without guidance for how to ensure appropriate security measures, many businesses will likely just implement the minimum safety standards that they can and hope that no breaches occur.

Enforcement

The CCPA and the GDPR also differ significantly in their enforcement mechanisms. Under the GDPR, independent Supervisory Authorities are responsible for overseeing, enforcing, and investigating data protection within the European Union. In addition, an independent European Data Protection Board oversees operations throughout the Union and is tasked with ensuring that the GDPR is consistently applied throughout the Union and providing guidance where needed.

Under the CCPA, enforcement is tasked to the California Attorney General, who must be notified of any actions brought against a business. Once notified, the Attorney General can decide to prosecute against the violation, but if he or she decides not to take action then the burden falls onto the consumer to continue the action (further adding cost and burdens to the consumers). In addition, once notified of a violation, a business is given thirty days to become CCPA compliant, and if it manages to do so, will not be considered in violation of the CCPA.

---

[1] A business's response to a data breach (involving PII) is governed by a separate data breach notification law, CA. CIV. CODE § 1798.82.

Conclusion

While the California Consumer Privacy Act of 2018 is certainly a step in the right direction for data privacy in the United States, there are still some serious improvements that must be made before it can truly be considered a GDPR 2.0. While it does allow for transparency of what PII is being collected from consumers, it does not go far enough in giving them control over how that information is used and processed by businesses. The broad exceptions of the CCPA, without further clarification, give too much freedom to businesses to take advantage of consumers' personal data, while still imposing significant burdens on small and medium businesses who hope to do business in the state.

That does not mean that the CCPA will not benefit consumers, though. Between now and January 1, 2020, California legislators will likely amend the CCPA in order to better achieve its goals. Its passage may also encourage action by the Federal Government to pass national data privacy laws, in order to resolve the patchwork of state data privacy laws throughout the country.