Hogan Lovells
CHRONICLE of DATA PROTECTION
PRIVACY & INFORMATION SECURITY NEWS & TRENDS

Posted on October 3rd, 2018 By Bret Cohen, Britanie Hall and Ryan Woo

California Consumer Privacy Act: The Challenge Ahead – A Comparison of 10 Key Aspects of The GDPR and The CCPA

This is the fifth installment in Hogan Lovells' series on the California Consumer Privacy Act.

As the most comprehensive privacy law to be enacted in the United States thus far, the California Consumer Privacy Act (CCPA) has inevitably invited comparisons to the European Union's General Data Protection Regulation (GDPR). At first glance, it is clear that the drafters of the CCPA (and the ballot measure that spurred its passage) drew inspiration from the GDPR. However, the CCPA is not a carbon copy of the GDPR, and a GDPR compliance program will not automatically meet the requirements of the CCPA. As businesses begin their CCPA compliance efforts, awareness of these laws' similarities and differences will be key to creating efficient and effective compliance programs that capitalize on prior GDPR compliance work but also address the unique nuances of the CCPA. This post compares the CCPA and the GDPR in ten key areas: (1) geographic scope, (2) entities subject to the law, (3) the definition of personal data/information, (4) notice requirements, (5) access and portability rights, (6) deletion rights, (7) rights to object or opt out, (8) relationships with processors/service providers, (9) anti-discrimination / compelled consent provisions, and (10) enforcement.

1. Geographic Scope

Both laws can apply to entities located inside and outside of their respective jurisdictions. The GDPR applies to entities that are established in the EU, as well as entities not established in the EU that process the personal data of persons located in the EU in the context of either (i) offering goods or services to persons in the EU, or (ii) monitoring the behavior of persons in the EU.

While the CCPA is less explicit about its geographic scope, it will likely also have extraterritorial effect. The statute's most direct reference to geography comes in the definition of "business" (the class of entities which are

subject to most CCPA requirements), which requires that an entity subject to the law "does business" in California. While the CCPA does not define this phrase, "doing business" has a long history of interpretation under U.S. and California personal jurisdiction jurisprudence. Therefore, the CCPA should apply to any business, regardless of physical presence or place of incorporation, which regularly offers goods or services to persons or entities in California or otherwise purposefully derives benefit from its activities in California.

2. Entities Subject to the Law

The GDPR and CCPA take different approaches to defining the types of entities that must comply with the law. Under the GDPR, any person or entity that processes (collects, stores, uses, etc.) personal data can be subject to the law's requirements, unless such processing is for purely personal or household purposes. Whether an organization operates for profit, meets certain revenue thresholds, or collects personal data from a certain number of persons has no bearing on GDPR's application.

In contrast, the CCPA sets out a number of threshold criteria for what type of entity constitutes a covered "business," namely that it: (1) operates for profit, (2) collects California consumer personal information, (3) determines the purposes and means of processing that information, and (4) meets one of the following criteria: (i) has annual gross revenues exceeding $25 million, (ii) annually buys or sells personal information of 50,000 or more California consumers, households, or devices, or (iii) derives more than 50% of its annual revenue from selling California consumers' personal information. Alternatively, an entity can qualify as a "business" if it controls or is controlled by an entity that meets the above criteria and shares common branding with that entity. Thus, a non-profit organization—which can be subject to the GDPR—would not be directly subject to the CCPA unless it controls or is controlled by a for-profit entity that qualifies as a "business" and shares common branding, or receives personal information from a business via a "sale."

3. Definition of Personal Data/Information

The GDPR and CCPA have similar definitions of personal data/information that are conditional, content-neutral, and can potentially cover any type of information, provided there is a sufficient link between the information and a particular individual. The GDPR defines personal data as "any information relating to an identified or identifiable natural person." Personal information under the CCPA is "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." A notable difference between these definitions is the CCPA's inclusion of information linked to a particular "household." While not defined in the CCPA, a "household" will likely cover, at minimum, data linked to a particular address, even if such data is not linked to any natural persons or device identifiers.

4. Notice Requirements

The GDPR and CCPA have partially overlapping notice requirements. Among other things, the GDPR requires that controllers notify data subjects about the purposes for which personal data will be processed, the legal basis for processing, the categories of entities who may receive the personal data, the retention period for personal data, and the data subjects' rights. This information must be provided to data subjects at the time when personal data are collected (if data is collected directly from a data subject), or within a reasonable period after the data is collected (if data is collected from a source other than the data subject).

The CCPA requires that businesses notify consumers prior to or at the point of collection only of the categories of personal information collected and how it will be used. Unlike the GDPR, the CCPA does not specify how or when such notice should be provided if a business collects personal information from a source other than the consumer and never has contact with the consumer. The GDPR allows this notice to be provided "within a reasonable

period of time" or, if used for communication, at the time of first communication, and provides an exception to notice where doing so would prove impossible or involve a disproportionate effort.

The CCPA does require businesses to disclose a significant amount of information in their online privacy policies, including some categories not required by the GDPR. In particular, the CCPA requires a business's online privacy policy to disclose a description of CCPA rights and how to exercise them, as well as three separate lists of the categories of consumer personal information that the business, over the preceding 12 months, has (1) collected, (2) sold, or (3) disclosed for business purposes (or the fact that it has not done so).

5. Access and Portability Rights

Both laws have relatively similar access and portability rights, although the scope of the CCPA's portability obligation is arguably broader.

The GDPR access right grants data subjects the right to obtain confirmation of whether a data controller is processing their personal data, access to the personal data itself, and general details about the processing. The GDPR also provides a separate right to data portability, under which the data subject has the right to receive the personal data that she provided to a controller in a "structured, commonly used and machine-readable format" and to transmit such data to another controller without hindrance. However, such data portability is limited to personal data processed on the basis of consent or on a contract, where the processing is carried out by automated means.

Although the CCPA and GDPR access rights are similar in many ways, one key difference is the CCPA's requirement that a business list the categories of personal information that it sells/discloses to each category of third party to which the consumer's personal information is sold/disclosed. Given that the GDPR does not explicitly require this granular information about third party disclosures, businesses that have already prepared for GDPR access requests may need to take additional steps to map and maintain ongoing awareness of how each individual consumer's personal information is transferred to third parties.

In addition, under the CCPA, information provided in response to an access request may be delivered by mail or electronically, and if provided electronically, must be "in a portable and, to the extent technically feasible, in a readily usable format that allows the consumer to transmit this information to another entity without hindrance." As such, the CCPA requires the portability of all personal information, and unlike the GDPR does not limit portability just to personal data both provided by the data subject and processed on the basis of consent or contract.

6. Deletion Rights

The GDPR and CCPA both grant individuals the right to have their data deleted under certain circumstances. The GDPR deletion right is limited to enumerated situations, such as when personal data are no longer necessary for the purposes for which they were collected or when processing is based on consent that has subsequently been withdrawn. Additionally, there are broad exceptions that allow a data controller to refuse to delete data (e.g., data is necessary for compliance with a legal obligation).

While the CCPA's deletion right it is not limited to specific, enumerated situations, it is subject to several explicit but broadly framed exceptions for certain uses of personal information. For example, a business can refuse to delete information that is necessary to provide the service, complete a transaction, detect security incidents or fraud, or for "solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.".

Given the fundamental similarities between the GDPR and CCPA deletion rights, businesses that have developed GDPR deletion policies and procedures will likely be able to repurpose these documents when designing the analogous CCPA policies and procedures. However, such policies will need to be revised to account for the different considerations that are involved in determining whether a deletion request must be honored. For example, the GDPR may require a business to consider alternative legal bases for processing if a data subject withdraws consent, such as the company's legitimate interest in retaining the personal data for security purposes, while the CCPA will require the business to determine whether any of the use exceptions apply. On balance, the CCPA's exceptions to the deletion right are more straightforward than the GDPR's exceptions. However, some of the CCPA exceptions will still require thoughtful analysis (e.g., considering whether data is used for purposes that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business).

7. Rights to Object/Opt Out

Consumers' broad right to opt out of the sale of their personal information is one of the most impactful elements of the CCPA. As discussed in our previous blog post, the term "sale" is broadly defined and will likely encompass many types of data sharing between entities. The CCPA does not list any exceptions to this right to opt out.

While the GDPR does not have a direct analog to the CCPA's right to opt-out of the sale of personal information, the GDPR's right to object affords data subjects an unconditional right to stop the use of their personal data for direct marketing purposes. The unconditional nature of the right to stop direct marketing makes this right somewhat analogous to the CCPA's right to opt out of the sale of personal information. Moreover, under Article 21 of the GDPR, a data subject can object to the processing of personal data under the controller's "legitimate interests" unless the controller demonstrates compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject. Although it is yet to be seen how EU regulators will interpret the scope of this objection right, certain data-sharing relationships that overlap with the CCPA's concept of "selling" data will most likely be encompassed. (For more on this, see our future blog post on the impact of the CCPA on data-sharing relationships.)

Therefore, policies and procedures that have been developed to implement the GDPR's direct marketing opt-out —or other consumer choices—may be of use when designing policies and procedures to implement the CCPA's sale opt-out. However, these policies and procedures will need to be revised in order to account for the fact that the "sale" opt-out will apply to a broad range of activities beyond direct marketing (e.g., sharing personal information with a third party for their own analytics purposes).

The CCPA also requires that a business that sells personal information must provide a "clear and conspicuous link" titled "Do Not Sell My Personal Information" on the business's homepage that enables a consumer or a person authorized by the consumer to opt out of the sale of the consumer's personal information. Mere inclusion of such a button on a business's homepage could lead more California consumers to exercise their right to opt out than EU end users, whose right to opt out needs to be explained only in a privacy policy. Therefore, businesses may wish to consider whether to offer a California-specific version of their homepage or how they will deal with non-Californian consumers who click on that link.

8. Relationships with Processors/Service Providers

Both laws have implications for service provider relationships. However, the GDPR imposes more explicit and extensive obligations for data processors than the CCPA.

Under the GDPR, transfers of personal data to processors (pure service providers) must be governed by a contract that expressly requires the processor to, among other things, process personal data only on the documented instructions of the controller, ensure that persons authorized to process personal data are bound by

a duty of confidentiality, provide appropriate technical and organizational measures for security of personal data, and assist the controller with other GDPR requirements. Processors may retain sub-processors only with the consent of the controller and must flow down their GDPR obligations.

By contrast, the CCPA does not mandate that a business impose specific contractual obligations on its service providers. Rather, the CCPA incentivizes businesses to impose certain contractual limitations on service providers by creating an exception to the definition of "sale" for transfers of consumer personal information to them. To take advantage of this exception, a business must execute a written contract with the service provider that prohibits the service provider from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing services specified in the contract for the business or as otherwise permitted by the CCPA. To avoid compliance obligations and liability under the CCPA itself, the service provider may not further collect, sell, or use the personal information provided by the business, except as necessary to perform the business purpose specified in its contract.

Although not explicitly required by CCPA for service provider contracts, businesses will also want to consider contractually requiring service providers to facilitate the fulfillment of deletion requests given that the CCPA requires businesses to "direct any service providers to delete the consumer's personal information from their records" if requested by the consumer. And, to the extent a service provider also holds personal information subject to a consumer access right under the CCPA, businesses will also want to contractually obligate their service provider to assist with such requests, including to provide a copy of such information in a portable and "readily usable" format.

Companies subject to both the GDPR and CCPA should consider updating their contracting processes to account for the new issues raised by the CCPA. This could involve revising existing privacy/confidentiality language in service provider contracts to extend existing protections to cover California personal information or adding terms that specifically address CCPA requirements for just California personal information.

9. Anti-Discrimination / Compelled Consent

Businesses are prohibited from discriminating against consumers who exercise their rights under the CCPA. Discrimination is broadly defined to include denying, charging different prices for, or offering different qualities of goods or services. However, the CCPA does allow businesses to charge consumers different prices or offer different qualities of goods or services if the difference is "reasonably related to the value provided to the consumer by the consumer's data."

Although the GDPR does not have a direct analog to the CCPA's anti-discrimination requirements, the EU views the right to privacy as a fundamental human right that cannot be waived by consent. Thus, by implication, a user contract that required the data subject to waive their GDPR rights as a condition to use a service would be presumptively invalid. In addition, there is a significant debate under the GDPR about the extent to which a company can make the provision of a service conditional on consent to certain processing of personal data. Companies who have considered this issue under the GDPR may need to adapt their GDPR consent strategies to account for the CCPA's anti-discrimination provision.

The practical implications of the anti-discrimination provision on data strategies will be discussed in more detail in a future blog post in our CCPA series.

10. Enforcement

The GDPR and the CCPA both allow for significant fines. The GDPR caps fines at the greater of €20 million or 4% of worldwide turnover. The CCPA allows for fines of up to $2,500 per violation or $7,500 per intentional

violation, but notably does not place a cap on the total amount of fines. Unlike the GDPR, the CCPA provides businesses with a period of 30 days to cure alleged violations of the law before a fine can be assessed.

The CCPA and GDPR both include private rights of action. However, unlike the GDPR, which gives data subjects a right to a judicial remedy and compensation for damages from a controller or processor that infringes their rights, the CCPA offers a private right of action only to consumers whose personal information is subject to unauthorized access and exfiltration, theft, or disclosure as a result of a business's violation of its duty to implement reasonable security procedures appropriate to the nature of the information. Additionally, this right applies only to a subset of "personal information" (e.g., Social Security number, driver's license number, medical information, and other information subject to California's breach notification statute), and it does not apply if the personal information is redacted or encrypted.

Click here to read the next post in the CCPA blog series.

Hogan Lovells US LLP
555 Thirteenth Street, NW
Washington, DC 20004 | USA
Phone: +1 202 637 5600
Fax: +1 202 637 5910

Hogan Lovells International LLP
Atlantic House
Holborn Viaduct
London EC1A 2FG
United Kingdom
Phone: +44 20 7296 2000
Fax: +44 20 7296 2001