October 3, 2018

California's New Privacy Statute: Is It a US GDPR?

Advisory

By Nancy L. Perkins, Anthony Raglani, Zoe V. Walkinshaw, Ronald D. Lee, Angel Tang Nakamura, Anthony J. Samson

On September 23, 2018, the governor of California signed into law an amended version of the California Consumer Privacy Act of 2018 (CCPA),[1] which was originally enacted in late June 2018. The amendments are a partial response to extensive criticism of the legislation as overbroad, ambiguous, and excessively burdensome for organizations doing business in California. Throughout the summer, a coalition of businesses and industry associations (including the California Retailers Association, the Consumer Technology Association, the Internet Association and others), engaged in a concerted effort to persuade the California Legislature to clarify certain definitions in the law, limit its scope to prevent unintended consequences and delay its enforcement date to give regulated businesses the requisite time to establish systems and policies for compliance.[2] The Legislature's response addresses a few, but by no means all, of the industry's concerns. It delays enforcement of most of the law's provisions until July 1, 2020 or six months after the California attorney general publishes final implementing regulations,[3] whichever is earlier, and it clarifies certain exemptions from the law's reach, but it leaves intact a host of complex requirements. Any entity subject to the CCPA that interacts with individual consumers faces a considerable task in readying for compliance during the approximately 18-month period before the CCPA is enforced.

The CCPA is being heralded by many as a "first in the nation" privacy regime. Because it defines the "personal information" subject to its protection extremely broadly, and because it grants consumers extensive rights to control that information, it has been referred to as a US state's importation of the European Union (EU) General Data Protection Regulation 2016/679 (GDPR) that became enforceable on May 25, 2018. Many organizations that spent months or even years preparing to comply with the GDPR are considering whether those efforts will be sufficient to ensure compliance—or at least to bring them close to compliance—with the CCPA as well. But despite core similarities between the GDPR and the CCPA, having prepared for compliance with the former will not relieve a business of additional work to achieve compliance with the latter. Although GDPR compliance may help with some aspects of CCPA compliance, an assessment of the CCPA's requirements needs to be undertaken as a separate exercise and will require adopting new operational and policy measures.

[1] 2017 California Assembly Bill No. 375, California 2017-2018 Regular Session (amending Part 4 of Division 3 of the California Civil Code), amended by 2017 California Senate Bill No. 1121.

[2] *See* Coalition Letter.

[3] The CCPA directs the attorney general to adopt a number of regulations to further implement and clarify the scope and requirements of the law prior to its effective date. This may include the expansion or modification of the definition of protected "personal information," the adoption of additional exceptions as may be required for businesses to comply with state or federal law, and the implementation of rules and procedures governing the mechanics of the CCPA's opt-out and consumer-notice requirements. The attorney general is also granted the discretion to adopt additional regulations that are deemed to be necessary to the law's implementation.

Key Differences Between the CCPA and the GDPR

As a threshold matter, there are certain core differences between the CCPA and the GDPR in terms of the scope of regulated persons, information and activities. For example:

Covered Entities. The GDPR has broad application to any person or entity, regardless of location or nationality, that acts as a "controller" (i.e., a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data) or a "processor" (i.e., a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller) of personal data of individuals that is collected in connection with a presence in the EU. The CCPA is not so broad; it regulates a "business," defined as a for-profit legal entity that does business in the state of California and which:

1. Has annual gross revenues in excess of $25 million,
2. Alone or in combination buys, receives, sells or shares for commercial purposes the personal information of 50,000 or more consumers, households or devices on an annual basis, or
3. Derives 50 percent or more of its annual revenues from selling consumers' personal information, to provide consumers with a variety of rights with respect to the protection and control of their personal information.

This difference in covered entities reflects the fundamental underpinnings of the two laws: The GDPR is grounded on the principle that, in the EU, privacy is a human right. Although the California Constitution similarly refers to the right to privacy as among the "inalienable" rights of all individuals, the CCPA itself does not seek to protect that right outside the commercial arena. It is "consumers" whose personal data is protected under the CCPA, and it is *businesses*, not other persons, upon which California has imposed the CCPA's requirements.

Personal Information. The GDPR protects "personal data" which is "any information relating to an identified or identifiable natural person (or a "data subject")." The CCPA similarly protects "personal information," but the definition of that term is designed to cover not only information identifiable to an individual consumer, but also to consumers that purchase or use products or services jointly: "'Personal information' means 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*."

Importantly, however, as clarified by the recent amendments to the CCPA, certain information that is subject to protection under other US privacy regimes is exempt from the CCPA. For example, nonpublic personal financial information that is collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act and its implementing rules or the California Financial Information Privacy Act is also generally exempt from the CCPA (although a breach in the security of this information would be actionable in a private party suit brought under the CCPA). In addition, medical information governed by the California Confidentiality of Medical Information Act and "protected health information" collected or created by "covered entities" or

"business associates" as those terms are defined under the Health Insurance Portability and Accountability Act (HIPAA) and its implementing rules are not subject to the CCPA. Information is exempt if it is collected as part of a clinical trial subject to protection under (i) the so-called "Common Rule" protecting human research subjects; (ii) the parallel rules of the Food and Drug Administration, or (iii) good clinical practice guidelines issued by the International Council for Harmonization in research. This latter exemption, vigorously advocated for by the pharmaceutical and medical device industries, is critical to prevent risks to the integrity of clinical trials that would exist if consumers who are research subjects could request access to or deletion of their personal data collected in the course of a clinical trial in which blinded studies and consistent data retention are essential to accurate analysis and reliable results.

There is ambiguity—or perhaps a serious deficiency—in the exemption for research subject information, however, in that much research involving human subjects takes place outside of actual "clinical trials"—for example, through surveys, interviews and other channels. The specific reference to data collected in a "clinical trial"—as opposed to in human-subject research more generally—may not encompass information collected for purposes of, for example, pharmacoeconomic or outcomes research, or for purposes such as identifying clinical trial participants. The medical research community may wish to seek further clarifying amendments to foreclose the possibility of an adverse impact on such nonclinical research.

Core Consumer Rights. Most of the basic privacy rights protected by the CCPA and GDPR are similar. The CCPA declares the California Legislature's intent to ensure five core consumer rights of California residents with respect to personal information about them:

- the right to know what personal information is collected;
- the right to know whether that personal information is sold or disclosed, and to whom;[4]
- the right to "say no" to the sale of that personal information;
- the right to access that personal information; and
- the right to equal service and price, regardless of exercising their privacy rights.

The GDPR similarly grants individuals the right to notice of what types of personal information about them will be collected and disclosed, as well as the right to access the collected information. But unlike the CCPA, the GDPR does not focus specifically on the sale of personal data—the GDPR regulates "processing" generally, which encompasses collection, disclosure, sale, and the many other forms of activity that may occur with respect to personal data. And the GDPR does not require special notice of an individual's right to block the sale of personal information, whereas the CCPA requires each regulated business to post a clear and conspicuous notice on the homepage of its website of a consumer's right to prevent such sale, which must be an active link for consumers to click stating: "Do Not Sell My Personal Information." (For children, the CCPA requires

[4] The CCPA requires a business that collects a consumer's information to disclose to that consumer the categories and specific pieces of personal information that the business has collected, sold to a third party or disclosed for a business purpose, as well as the categories of third parties with whom the business has sold or disclosed personal information, among other items. Businesses must also disclose the categories of the sources from which personal information has been collected and identify the business or commercial purpose(s) underlying the collection of consumers' information. The CCPA establishes specific requirements for the form and timing of delivery of information requested by a consumer.

additional protection: children under the age of 16 must affirmatively ***opt-in*** before businesses can sell their personal data, and parents of children under the age of 13 must *opt-in* on the child's behalf.)

Deletion of Personal Information. Another area in which the GDPR and CCPA are similar, but different enough to suggest distinct practices and policies, concerns the right of individuals to have their personal information deleted upon request. Under the GDPR, such a request must be honored in any of six circumstances, including when the personal information is no longer necessary in relation to the purposes for which it was processed or the individual has withdrawn their consent to processing and there is no other legal ground for processing. The CCPA, while establishing a general right to deletion, narrows the right substantially by permitting a business to decline an individual's request for deletion of certain personal information under nine specific conditions, including if the business needs to keep that information to "enable solely internal uses that are reasonably aligned with the expectations of the individual based on the individual's relationship with the business" or to "[o]therwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information."

Third-Party Processing Contracts. Another noticeable difference between the CCPA and the GDPR is that the GDPR requires any "controller" that shares personal information with a third-party "processor" to enter into a contract with the processor that places specific data protection obligations on the processor. Although other privacy laws in the United States, including the HIPAA privacy regulations and the Gramm-Leach-Bliley Act rules, impose such contractual obligations on "covered entities" and financial institutions, respectively, the CCPA does not require the businesses it regulates to similarly bind third-party processors to data protection obligations.

A more detailed summary of the similarities and differences between the CCPA and the GDPR is set forth in chart form below. As the summary indicates, while the CCPA and GDPR both are expansive pieces of legislation that similarly extend certain privacy rights to individuals in relation to their personal information, each law has subtleties in its definitions, mandates and exceptions that critically impact its application and interpretations. Businesses seeking to comply with both laws should view compliance with the CCPA as a separate phase of their data privacy program, albeit a phase that is following closely on the heels of, or is in conjunction with, their GDPR compliance. The specific details of both laws should be fully assessed so that business practices and policies can be implemented and adjusted accordingly.

Summary Comparison of Key Provisions of the CCPA and the GDPR

Provision	CCPA	GDPR	Practical Implications
Covered Entities	A "business" is defined as any for-profit legal entity that does business in the state of California and collects and controls consumers' personal information and satisfies one or more of the following thresholds: (1) annual gross revenues in excess of $25 million, (2) alone or in combination buys, receives, sells or shares for commercial purposes the personal information of 50,000 or more consumers, households or devices on an annual basis, and (3) derives 50 percent or more of its annual revenues from selling consumers' personal information. A "business" also includes any entity that controls or is controlled by a business that satisfies these criteria.	Applies to processing of personal data by: 1. A "controller," i.e., a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; or 2. A "processor," i.e., a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.	The CCPA is not intended to apply to smaller companies, but apart from the $25 million revenue threshold, the remaining prongs of the definition are somewhat unclear, for example, due to the breadth of certain underlying terms, such as "sell," and the inclusion of terms such as "households" and "devices," each of which could plausibly be located outside of California.
Scope	Can apply to businesses located outside of California if personal information of California consumers is collected.	Can apply to processing of personal data relating to EU or non-EU data subjects in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not. Can apply to processing of personal data of EU data subjects by controllers or processors located outside of the EU if the processing activities are related to the offering of goods/services to, or monitoring the behavior of, individuals residing in the EU.	The protections of the CCPA are anchored to California residents. Accordingly, any business that "does business" in California, regardless of its physical location, may become a covered entity due to its interaction with California residents.

Provision	CCPA	GDPR	Practical Implications
Protected Individuals	"Consumers" are protected and are defined as any natural person who is a California resident. By contrast, "persons" such as other individuals not meeting the definition of consumer, sole proprietorships, partnerships, LLCs, corporations, and a variety of other legal entities are not protected.	Any "data subject," which is defined as "an identified or identifiable natural person." An "identifiable natural person" is defined as "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."	The CCPA's definition of "consumer" could be read to apply to individuals involved with commercial transactions or functions, including employees of businesses involved in such activities. This would appear to extend the reach of the CCPA beyond its intended scope and could create unintended consequences for businesses engaged in routine commercial functions with no personal, family or household purpose.

Provision	CCPA	GDPR	Practical Implications
Protected Information	"Personal information" 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. It includes, but is not limited to, the following: (1) identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers; (2) categories of information described under Cal. Civ. Code § 1798.80; (3) characteristics of protected classifications under California or federal law; (4) commercial information; (5) biometric information; (6) internet or electronic network activity information; (7) geolocation data; (8) audio, electronic, visual, thermal, olfactory or similar information; (9) professional or employment information; (10) education information; and (11) inferences drawn from any of the above information to create a consumer profile. "Personal information" does not include any publicly available information.[5]	"Personal data" or "any information relating to an identified or identifiable natural person (or "data subject")."	The CCPA's definition of "personal information" is exceptionally broad. In effect, the CCPA protects any identifying information about a consumer or which could reasonably be linked to a consumer, as well as any identifying information that relates to a *household*. The term "household" is not defined, but could plausibly include residences outside of the state of California owned or rented by or otherwise housing California residents, as well as any connected devices within those households that contain personal information about California residents. Without clarification, the inclusion of the term "household" could be used to further broaden the already-considerable amount and types of information protected by the CCPA.

[5] This definition provided in this chart has been abbreviated to include only its essential elements. The statutory definition contains additional guidance regarding certain categories of "personal information" and certain terms included within the definition are defined separately under the statute.

Provision	CCPA	GDPR	Practical Implications
Definition of "Processing"	Any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	
Definition of "Sell"	Selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.	Not a separate concept; would be included in the definition of "processing."	The CCPA's definition of "sell," like many other key terms, is very broad and includes acts such as "disclosing" personal information in exchange for "other valuable" (i.e., potentially nonmonetary) consideration. Accordingly, a business' disclosure or transfer of personal information to a third party in connection with a broader transaction or services agreement may be sufficient to constitute a sale.
Definition of "Collect"	Buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. The definition includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.	Not a separate concept; included in the definition of "processing."	The CCPA's definition of "collect" is both broad and ambiguous. The term would capture a business' *passive receipt* of personal information, regardless of the factual context or means of delivery and receipt. Many significant business functions, such as marketing, service provider management and acquisitions, will almost certainly involve the "collection" of personal information as it is currently defined.

Provision	CCPA	GDPR	Practical Implications
Information Requirements	Upon receipt of a consumer's request for any disclosure of the categories and specific pieces of personal information that a business has collected about that consumer, the business must deliver such information to the consumer free of charge within 45 days of receipt of a verifiable request. The time period for disclosure may be extended once by an additional 45 days upon the provision of notice to the consumer. The delivery of information can be made by mail or electronically; however, electronic disclosures must be provided in portable format to the extent feasible. Businesses that collect a consumer's personal information are required, either at or before the point of collection, to inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. Businesses are not permitted to collect additional categories of personal information, or use collected information for additional purposes, without providing notice to the consumer.	A list of information needs to be provided to data subjects (1) at the time their personal data is obtained if their personal data was collected directly from them, or (2) within certain timeframes afterwards if their personal data was not collected directly from them. In the second case, certain limited exemptions to the information requirement apply, such as that its provision would be impossible or involve a disproportionate effort. The list of information to be provided includes the identity and contact details of the controller, the contact details of the data protection officer, the purposes for processing and legal basis/es for processing, the recipients of the personal data, the personal data retention period, the data subjects' rights, and appropriate safeguards used to transfer the personal data out of the EU.	The CCPA's requirement that businesses provide consumers with "specific pieces" of information is not defined or explained. Even absent any ambiguity, from an operational perspective, many businesses will be challenged to design and implement systems and controls capable of delivering the "specific pieces" of information intended to be covered by the law. In addition, this provision will require businesses to transmit sensitive information, thereby exposing the information, perhaps unnecessarily, to security risks. Any increased exposure to a potential security breach is, for a variety of reasons, problematic for businesses. Here it is worth noting, as discussed further below, that the CCPA's private right of action provision can be triggered by a security breach involving a consumer's personal information.

Provision	CCPA	GDPR	Practical Implications
Consent Requirements	In order to comply with consumer opt-out provisions, businesses must make available two or more designated methods for submitting requests for disclosure of information including, at minimum, a toll-free telephone number and a public website. Business' websites must provide a clear and conspicuous link on their websites titled "Do Not Sell My Personal Information" that enables consumers to opt-out of the sale of their personal information. In addition, businesses must provide a description of consumers' right to opt out of the sale of their personal information, along with the above-described website link, in their website privacy policies or in any California-specific description of consumers' privacy rights. Businesses must also disclose in a form that is reasonably accessible to consumers and in accordance with a specified process that consumers have a right to request that their personal information be deleted.	Consent is one legitimate ground for processing personal data and several others apply. If a controller or processor wants to rely on consent, and not another ground, it needs to be aware that the threshold for valid consent is high. Opt-out consent is not valid. Consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." Consent requirements are without prejudice to the requirements under the EU Privacy and Electronic Communications Directive 2002/58/EC (currently being updated) to obtain consent to send certain forms of electronic marketing to individuals.	The CCPA's opt-out provision is inflexible in that it requires a consumer to either opt-out of *all* sales of his/her personal information, or permit such sales in their entirety. Consumers may determine that they benefit from certain types of sales or transfers of their personal information, but they will not be able to permit certain sales while prohibiting others. Moreover, given the breadth of the CCPA's definition of "sell," a consumer's opting out of the sale of his/her personal information may have consequences that are unknown to the consumer, such as limiting the business' ability to transfer the information between business units or to service providers, which could in turn limit the utility of the services received by the consumer.
Data Retention Requirements	Businesses are not required to retain any personal information collected for a single, one-time transaction if the information is not sold or retained by the business. Businesses that sell personal information must be prepared to provide disclosures to consumers regarding the collection and use of their personal information covering the preceding 12-month period from the date of receipt of the request.	Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, with certain limited exceptions. Information about the period for which personal data will be stored, or if that is not possible, the criteria used to determine that period, needs to be included as part of the information requirements (see the "Information Requirements" section above).	Although the CCPA does not prescribe minimum record-retention periods for consumers' personal information, in effect, the CCPA will require businesses to retain information in order to preserve the ability to disclose such information to consumers if requested. In certain instances, businesses may be required to retain information for much longer than would be necessary in the ordinary course of business.

Provision	CCPA	GDPR	Practical Implications
Rights Granted to Protected Individuals	Establishes four core individual rights: (1) The right to request that a business deletes personal information that it has collected about a consumer. (2) The right to request and receive information about, and specific pieces of, personal information that has been collected or sold or disclosed to third parties by a business. (3) The right to opt out of the sale of a consumer's personal information. (4) The right to not be discriminated against due to the exercise of any right established by the CCPA.	As the CCPA does, the GDPR establishes the rights in points (1) and (2) of the opposite column, though the exemptions to these rights differ between the CCPA and GDPR. The GDPR does not establish the rights in points (3) and (4) of the opposite column. The GDPR additionally establishes the rights for data subjects who may, with regard to their personal data (under certain circumstances): • request it to be rectified; • have its processing restricted; • have it provided to them and transferred to another organization; • object to its processing; • withdraw their consent to its processing; • complain to a regulator about its processing; and • not be subject to a decision based solely on certain forms of automatic processing, including profiling.	Several of the practical implications of the consumer rights established by the CCPA are discussed elsewhere in this chart; however, with respect to the deletion of personal information, the CCPA overlooks several practical issues presented by this requirement. For example, in many instances, particularly in sectors that involve significant amounts of data processing, consumers' information may be organized and maintained in ways that will make it challenging for a business to retrieve and delete the information of a single consumer upon request. In addition, the CCPA does not account for varying uses of personal information and the related impact of the deletion of such information. A consumer could, for example, request the deletion of personal information that is relevant to a workplace investigation involving that consumer or which is critical to the due diligence of a pending commercial transaction—in both instances undermining a use of the information that was likely unintended. Also of note, the recent amendments to the CCPA include a provision limiting the rights of consumers and the obligations of businesses to the extent that they infringe on any noncommercial activity of a covered entity. This provision was likely added in an effort to limit the potential for free speech challenges to the law under either the US or California Constitutions.
Opt-Out Provisions	A business that sells consumers' personal information must disclose this fact to consumers, who have the right to opt out of the sale of their personal information. For consumers under the age of 16, the parents of the consumer have the right to opt-in to any sale of the consumer's personal information.	A directly comparable obligation does not exist; however, data subjects can try to enforce their rights (as described in the row above) with regard to any selling of their personal data.	With respect to the CCPA's opt-out provisions, see above discussion regarding the mechanics and utility of the provision.

Provision	CCPA	GDPR	Practical Implications
Remedies	The CCPA establishes a private right of action for any consumer whose nonencrypted or nonredacted personal information was subject to an unauthorized access and exfiltration, theft or disclosure as a result of a business' failure to implement and maintain reasonable security procedures. Statutory damages are limited to not less than $100 and not more than $750 per consumer per incident, as well as injunctive and declaratory relief and any other relief deemed proper by the court. The CCPA also provides for administrative enforcement, including by authorizing the attorney general to bring actions for civil penalties against any business that fails to cure an alleged violation of the law within 30 days of being notified of such violation. Civil penalties of $2,500 per violation or $7,500 per intentional violation may be imposed by the attorney general. The attorney general is not authorized to bring an enforcement action until the earlier of six months after the date of publication of final regulations issued as required by the CCPA or July 1, 2020.	Data subjects have the following rights: (1) Right to a judicial remedy against a legally binding decision of a regulator. (2) Right to a judicial remedy against a controller or processor. (3) Right to compensation from a controller or processor. Regulators can also impose fines on controllers or processors of up to the higher of €20 million or four percent of total worldwide annual turnover of the preceding financial year for the most serious breaches of the GDPR.	The CCPA's private right of action provision applies if a consumer's "nonencrypted *or* nonredacted" personal information was the subject of a security breach or other form of unauthorized access. The use of "or" rather than "and" is likely a drafting error; however, at present the language has the effect of broadening the scope of the provision. Irrespective of whether this language of the law is clarified, in light of the breadth of the CCPA's key operative terms and provisions, the private right of action authority is likely to lead to a significant amount of class action litigation in connection with security breaches involving protected personal information.

People

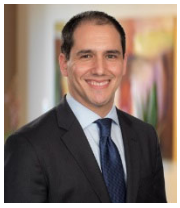
Nancy L. Perkins
Counsel, Washington, DC
+1 202.942.5065
nancy.perkins@arnoldporter.com

Anthony Raglani
Associate, Washington, DC
+1 202.942.5482
anthony.raglani@arnoldporter.com

Zoe V. Walkinshaw
Associate, London
+44 (0)20 7786 6122
zoe.walkinshaw@arnoldporter.com

Ronald D. Lee
Partner, Washington, DC
+1 202.942.5380
ronald.lee@arnoldporter.com

Angel Tang Nakamura
Partner, Los Angeles
+1 213.243.4094
angel.nakamura@arnoldporter.com



Anthony J. Samson
Senior Attorney and Policy Advisor
+1 916.210.7999
anthony.samson@arnoldporter.com