A Slice of GDPR in California?

White & Case Technology Newsflash

The recently passed California Consumer Privacy Act of 2018[1] (the "**CCPA**") is set to create significant compliance burdens for most businesses that collect personal information about California residents ("**consumers**[2]").

The CCPA introduces new obligations on covered businesses, including to:

- disclose what personal information the business collects about consumers and to whom the business sells or discloses that personal information; and
- respect new rights for consumers, including rights to request access to and deletion of their personal information and to opt out of having their personal information sold to third parties.

Liability for failure to comply could easily reach millions of dollars in some circumstances: businesses may be subject to civil liability in the event of a data breach caused by a failure to implement and maintain reasonable security procedures and practices; and knowing violations of other provisions may subject a business to civil penalties up to $7,500 per violation.

The new requirements are likely to necessitate significant updates to covered businesses' external and internal privacy policies and operational compliance procedures, in particular, to enable them to respond to consumers who exercise their rights under the CCPA.

Certain provisions of the CCPA bear some similarities to the European Union's new General Data Protection Regulation[3] ("**GDPR**") and businesses that have put in place a GDPR compliance framework may, to a certain extent, be able to leverage their existing processes to comply with the CCPA. However, even where there are similarities between the two laws, the requirements also have subtle differences, requiring a careful analysis and application for businesses subject to both laws.

The CCPA takes effect on January 1, 2020, and the California Attorney General (the "**AG**") is anticipated to promulgate related regulations and guidance in the interim. However, the California legislature recently passed a bill ("**S.B. 1121**")[4] that, as well as clarifying potential ambiguities in the CCPA, would also extend the deadline for the AG to issue regulations, and delay enforcement of the CCPA until July 1, 2020 or later. The bill is currently awaiting the governor's signature. Businesses may participate in the public review and comment period for future regulations, once the open comment period has started,[5] by contacting the AG.

Steven R. Chabinsky
Global Data, Privacy & Cybersecurity

T +1 202 626 3587
E steven.chabinsky@whitecase.com

F. Paul Pittman
Global Data, Privacy & Cybersecurity

T +1 202 729 2395
E paul.pittman@whitecase.com

A Slice of GDPR in California?

Background

The CCPA builds on existing data privacy legislation in California including the "Shine the Light" law,[6] the California Online Privacy Protection Act,[7] and California's data breach notification law.[8] The CCPA was passed amid concerns that consumers cannot "properly protect and safeguard their privacy."[9] Its passage comes at a time when many US companies with international operations are still dealing with the significant compliance burden associated with the GDPR and, despite some similarities, the CCPA will place additional burdens on businesses that are subject to both laws.

Scope: Covered Entities, "Personal Information" and "Consumers"

The CCPA applies to for-profit legal entities (or sole proprietorships) that:

(i) do business in the State of California;

(ii) collect personal information of consumers;

(iii) determine the purpose and means of the processing of consumers' personal information; and

(iv) *either*

- have annual gross revenue over $25,000,000;
- buy, sell, receive or share for commercial purposes, the personal information of 50,000 or more consumers, devices or households, on an annual basis; or
- derive 50 percent or more of their annual revenue from selling the personal information of consumers.

Personal information is broadly defined as "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." The CCPA provides several examples of personal information, including real name, alias, IP address, biometric information, network activity information (e.g., browsing and search history), and geolocation data.

The CCPA applies to "consumers" which it defines as natural persons who are California residents. Although the CCPA references and appears designed to protect consumers in the commonly understood sense (i.e., recipients of a good or service), its broad definition may cover data obtained in other circumstances, such as data related to a business's employees who are California residents. The CCPA specifically identifies "employment-related data" as a category of personal information covered by the CCPA and the legislative findings mention "apply[ing] for a job" as one of the activities that is "almost impossible to do ... without sharing personal information." Additionally, the CCPA never states that it applies only to personal information collected in the course of a consumer transaction or expressly excludes personal information collected by an employer about its employees for employment purposes. The scope of the CCPA will likely be clarified through legislative amendment, regulation, or guidance from the AG.

Despite its potentially broad reach, the CCPA is not all encompassing. The CCPA does not apply to "commercial conduct" which takes place entirely outside of California. In addition, the CCPA is not intended to replace or supersede federal and state laws, nor does it apply to personal information collected pursuant to certain laws, such as the Health Insurance Portability and Accountability Act[10] and the Gramm–Leach–Bliley Act.[11] The CCPA also excludes "personal information" transferred as part of a merger, acquisition or other corporate transaction, subject to certain conditions including requiring notice to a consumer if the acquirer of the information plans to use it in a way that is inconsistent with the conditions under which it was originally collected. Notably, as explained in more detail below, the CCPA excludes certain types of requests that businesses rely on to lower their compliance burden.

A Slice of GDPR in California?

Compliance Obligations

The CCPA imposes substantial obligations on covered businesses.

Provide Prior Notice of Data Collection Practices

At the time of, or before collecting personal information, a business must inform consumers of the categories of personal information to be collected and the purpose for which each category of personal information will be used. This prior notice could be included in the business's external privacy policy, see further requirements below.

Update Privacy Policy

A business should disclose (and update at least every 12 months) in both its existing privacy policy and any California-specific privacy description:[12]

- a description of consumers' specific rights under the CCPA and the methods provided by the business for consumers to submit corresponding requests (including if the business sells personal information, a link to a "Do Not Sell My Personal Information" webpage).[13]
- lists, in respect of the preceding 12 months, of:
  - the categories of personal information collected, the sources from which such personal information was collected, the categories of third parties with whom such personal information was shared;
  - the business or commercial purpose for collecting or selling personal information; and
  - the categories of personal information disclosed (for a business purpose) or sold (or a statement that the business has not engaged in such sale or disclosure, if applicable).

Honor Consumer Requests

A business is under an obligation to honor consumer rights granted under the CCPA within 45 days.[14] The CCPA requires businesses to:

- Access: disclose the following, in relation to personal information it has collected about the consumer in the preceding twelve months: (a) the specific pieces of information collected; (b) the categories of information collected; (c) the categories of sources from which that information was collected; (c) the business or commercial purpose for collecting that information; and (d) the categories of third parties with whom that information has been shared, including information sold to third parties. The disclosure should be made in writing and delivered: through the consumer's account with the business, if they have one (if not they should not be asked to create one); by mail; or electronically, at the consumer's option if they do not have an account (in which case the information must be provided in a readily useable format that allows the consumer to easily transmit the information to another entity). Such requests are limited to two per twelve-month period.
  - The business must provide at least two designated methods for consumers to submit requests, including, at a minimum, a toll-free telephone number and a web page (if the business maintains a web site).
- Deletion: delete the personal information the business has collected from the consumer, subject to certain exceptions, including if the consumer's personal information is necessary for the business or service provider to: (a) provide a good or service requested by the consumer; (b) complete the transaction for which personal information was collected; or (c) perform a contract between the business and consumer.
- Opt out: if they sell personal information to third parties, refrain from selling a consumer's personal information (and not request that the consumer authorize the sale of their personal information for at least twelve months from the opt out).[15] The business must provide a clear and conspicuous link entitled "Do Not Sell My Personal Information" on its website that directs consumers to a webpage where they can opt-out.

A Slice of GDPR in California?

Prohibited Discrimination

A business must not discriminate against a consumer who chooses to exercise his or her rights under the CCPA, e.g., by increasing prices, or reducing the level or quality of goods or services for those consumers. This does not prevent a business from varying prices, or the level or quality of goods or services if the difference equates to the value provided to the consumer by the consumer's data. Businesses may (1) offer financial incentives such as payments to a consumer as compensation, for the collection, sale, and deletion of personal information, and/or (2) offer a different price, rate, level, or quality of goods and services to consumers "if the difference is related to the value of having a consumer's personal information."

Educate Personnel

A business is under an obligation to ensure that individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA are informed of all requirements, and how to direct consumers to exercise their rights..

Penalties

State Enforcement

The CCPA contains significant tools for enforcement. Violation of the CCPA would expose businesses to civil penalties of up to $7,500 per intentional violation in suits brought by the AG (or any other public entity with the authority to sue on the behalf of the people of California). Civil penalties for non-intentional violations will be limited to $2,500 or less per violation. Businesses will have 30 days to cure any alleged violations after being notified of non-compliance.

Consumer Actions

The CCPA grants a right for consumers to bring a civil action for statutory damages. However, this applies only in relation to data security breaches which arise out of a failure by a business to comply with its duty (under a separate law[16]) to maintain reasonable data security measures. This right extends to consumers whose unencrypted or non-redacted personal information (defined by that separate law, and more narrowly than in the remainder of the CCPA[17]) has been stolen or disclosed as a result of a business's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information. Statutory damages are the greater of $100-$750 per consumer per incident, and actual damages. As such, an applicable data breach, involving as little as 10,000 records, could subject a business to a million dollar plus damages claim.

Wider Context and Concluding Thoughts

Compliance in Practice

To be prepared in practice to comply with these obligations under the CCPA, businesses are likely to need to implement operational changes, for example so that, for a given California resident, they are able to identify all relevant personal information they hold, are able to provide a copy and/or delete it on request, and, to the extent they sell personal information, to refrain from selling that particular California resident's personal information.

Lack of Clarity

The CCPA is unclear on several issues and raises several questions. For example:

- What does it mean to "do business in the State of California"?[18]
- What is a "household" in the context of "personal information" as defined by the CCPA and does the scope of information covered by "households" include other individuals within a household or simply information relating to a physical location?[19]
- Do consumer rights extend to consumers who do not have a direct relationship with the business, but whose data the business has collected (from other consumers for example)?
- Do consumers' rights regarding their personal information extend beyond the business that collected the personal information to any vendors or other third parties that maintain the personal information?
- Who is liable for the subsequent sale of a consumer's personal information by a third party who purchased the personal information from a business?
- Are the rights and obligations created under the CCPA intended to apply to collection of personal information by employers about their employees?[20]

A Slice of GDPR in California?

Latest Developments

Before it takes effect on January 1, 2020, the CCPA calls for the AG to solicit public input in developing regulations and procedures for certain key provisions of the law. It is also likely to be revised by the California legislature.

For example, the California legislature recently passed S.B. 1121, which would make several changes to the CCPA. Along with technical corrections, S.B. 1121 would amend the CCPA to make clear that the private right of action only applies to data breaches. It would also extend the deadline for the AG to issue regulations under the CCPA from January 1, 2020 to July 1, 2020. Should S.B. 1121 become law, the CCPA would not be enforceable until the earlier of July 1, 2020 or six months after the AG publishes final CCPA regulations. The bill is currently awaiting the governor's signature.

Therefore, there are opportunities for businesses that are concerned about particular measures or uncertainty in the CCPA to influence its final form and related requirements and procedures. To participate in the AG's proposed rulemaking process, participants will generally have 45 days from the date of announcement of the proposed rulemaking to submit their comments, either via email, fax, postal address, or at a public hearing. To date, a Notice of Proposed Rulemaking has not been announced by the AG.

Businesses may also seek the advice of the AG on how to comply with the law, although (as of the date of this article), the AG has not provided a means by which businesses may solicit such advice.

Other data privacy regimes, including the GDPR

For a global business, the CCPA will add an additional regulatory burden on top of the significant compliance overhead from other data privacy regimes, in particular the GDPR[21]. Although certain provisions of the CCPA resemble certain provisions of the GDPR, even those similar provisions also include subtle differences. Therefore, while businesses may find that existing compliance frameworks developed under the GDPR are useful for preparing for compliance under the CCPA, this will not avoid the need for a review of and updates to these frameworks. For businesses that have already been dealing with the compliance demands of the GDPR, this news is unlikely to be welcomed.

A Slice of GDPR in California?

[1] Cal. Civ. Code § 1798.100-195.
[2] See further, below.
[3] Regulation 2016/679, O.J. L 119/1 (2016). For more information on the GDPR, please see White & Case's GDPR Handbook and related publications.
[4] S.B. 1121, 2017-18 Leg. (Cal. 2018).
[5] Regulatory proposals in the State of California must typically undergo a public comment period of at least 45 days. Any notice of proposed rulemaking will be published in the California Regulatory Notice Register.
[6] Cal. Civ. Code § 1798.83.
[7] Cal. Bus. and Professions Code §§ 22575-22579.
[8] Cal. Civ. Code § 1798.82.
[9] A.B. 275, 2017-18 Leg. § 2(c) (Cal. 2018).
[10] Pub. L. No. 104-191, 110 Stat. 1936.
[11] Pub. L. No. 106-102, 113 Stat. 1338.
[12] Or, if it does not maintain a privacy policy, on its website.
[13] See "Honor Consumer Requests" below.
[14] Subject to extension in limited circumstances.
[15] In relation to minors, businesses are prohibited from selling their personal information without having received consent (i.e., opt-in) and, in relation to consumers that the business has actual knowledge are under the age of 16, without having affirmative authorization for the sale: in the case of minors between the ages of 13 and 16, from the minor; and, in the case of minors under the age of 13, from the minor's parent or guardian.
[16] Cal. Civ. Code § 1798.81.5 ("Privacy: personal information").?
[17] "Personal information" under Cal. Civ. Code § 1798.81.5 includes only: an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: Social security number; driver's license number or California identification card number; account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional; an individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records; or a username or email address in combination with a password or security question and answer that would permit access to an online account. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
[18] The CCPA applies only to "sole proprietorship[s], partnership[s], limited liability company[ies], corporation[s], association[s], or other legal entit[ies] that [are] organized or operated for the profit or financial benefit of [their] shareholders or other owners . . . that do[] business in the State of California." Cal. Civ. Code §1798.40(c)(1).
[19] See "Scope: Covered Businesses; 'Personal Information'; 'Consumers'" above. The CCPA does not define what a "household" is. Personal information includes "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." Cal. Civ. Code § 1798.140(o)(1).
[20] See "Scope: Covered Businesses; 'Personal Information'; 'Consumers'" above.
[21] For a comparison of areas of overlap between the GDPR and the CCPA, **see here**.

Mark Williams, Law Clerk at White & Case, and Charles Miller and Kyle Levenberg, summer associates at White & Case, also assisted in the development of this publication.