Media coverage

California: What California's paradigm-shifting privacy law means for your business

Customer DataData ProtectionLegal ReformPrivacy Policy

On 28 June 2018, the California Governor, Jerry Brown, signed and enacted into law Assembly Bill 375 ('AB 375') as the California Consumer Privacy Act of 2018 ('CCPA'). Alan L. Friel and Niloufar Massachi, Partner and Associate respectively at Baker Hostetler, provide us with a break-down of the law, discussing key provisions, uncertainties and its implications for businesses' operations.

Chris Leipelt/Unsplash.com

Complying with the CCPA

The CCPA, a privacy law unprecedented in the US, which grants California residents a broad range of European-like rights when it comes to their personal information ('PI'), will become effective 1 January 2020. In short, Californians will have the right to demand that a business provide it with a transportable copy of their PI, delete their PI, not sell their PI, and provide them with consumer-specific information about PI collection and sharing[1]. Specifically, regulated businesses[2] need to become prepared to do the following:

Providing consumer notice

To comply with the CCPA, a business must track the PI it collects and disclose in its privacy policy and any California-specific privacy notices, or otherwise on its website:

> a list of the categories of PI collected in the preceding 12 months and the purposes therefore;
> a list of the categories of PI sold in the preceding 12 months (or if the business has not sold consumers' PI in the preceding 12 months, the business must disclose that fact); and
> a list of the categories of PI disclosed for a business purpose in the preceding 12 months (or if the business has not disclosed consumers' PI for a business purpose in the preceding 12 months, the business must disclose that fact).

A business must also disclose in its privacy policy, or otherwise in forms readily accessible to them:

> a description of consumers' rights under the CCPA;
> a link to the 'Do Not Sell My Personal Information' webpage; and
> two or more designated methods for submitting requests.

Responding to consumer requests for information

Upon a verified request from the consumer, a business must provide the following information to the consumer on an individualised basis (i.e. specific to his or her data):

- the categories of PI collected about that specific consumer;
- the categories of sources from which the PI is collected;
- the specific pieces of PI collected about that consumer;
- the business or commercial purpose for collecting or selling the PI;
- the categories of third parties (which includes differently branded affiliates, and possibly similarly branded affiliates) with which the business shares PI;
- for PI that is sold, the categories of the consumer's PI sold to what categories of third parties, and the categories of the consumer's PI sold to each applicable third party (again third parties likely include affiliates); and
- for PI that is disclosed for a business purpose, the categories of the consumer's PI that were disclosed.

The right to individualised information as set forth above, means that businesses will have to track this information on a data-subject-specific basis, which will require record keeping not previously necessary. However, the required look-back period is 12 months, so businesses should start maintaining this information as of January 2019 to be able to comply with requests made shortly after the CCPA goes into effect as of January 2020. A business must respond to a consumer's verified request for information within 45 days, though under certain circumstances an extension of up to an additional 45 days is possible. Further, it must provide at least two methods for submitting requests for information, and at least a toll-free number, and a website address (if the business has a site). A business cannot require the consumer to create an account, or in ordinary circumstances charge the consumer, as a condition of fulfilling the request.

In addition to accommodating consumers' information rights, the CCPA requires that a business must promptly take steps to disclose and deliver a copy of a consumer's PI if requested, by mail or electronically, and if electronically, in portable, and, to the extent feasible, in a readily useable format that allows the consumer to transmit the PI to another entity without hindrance. However, businesses are not required to provide PI to a consumer more than twice in a 12-month period, and the same 12-month look back appears to apply to data access and portability requests. Additionally, businesses are not required to retain PI collected for a single, one-time transaction, if this PI is not sold or retained by the business or to re-identify or otherwise link information that is not maintained in a manner that would be considered PI.

Consumer choice

In addition to the right to obtain information about, and copies of, their PI as outlined above, the CCPA gives consumers the ability to control their PI by limiting its sale and being able, subject to some exceptions, to delete it. A business must have a clear and conspicuous link on its internet homepage, titled 'Do Not Sell My Personal Information' that links to an opt-out mechanism enabling a consumer to opt-out of the sale of that consumer's PI. A business must cease selling PI upon request, and must not solicit opt-in for 12 months following an opt-out. Further, a business must obtain opt-in consent from those it knows are under 16 to sell PI, and consent must be from the parent or guardian if the consumer is under 13. A party that has been sold PI cannot resell it without first giving the consumer notice and an opportunity to opt-out. Finally, a business must be able to delete, subject to certain exceptions, a consumer's

PI upon request, including PI in the possession of service providers. The deletion right is effectively a right to limit use short of selling the data, such as for marketing purposes. The requirement that a business cause its service providers to delete data when the business receives a deletion request will require contractual commitments. The CCPA requires other contractual commitments to be obtained by service providers, and it should be noted that the CCPA treats vendors engaged for operational business purposes and those engaged for commercial purposes differently, and the businesses' obligations and liability with respect to each differs materially.

The CCPA treats PI and its sale broadly

Beyond affording California residents broad rights regarding their PI, the law takes a very expansive view of what constitutes PI. The CCPA will regulate 'personal information,' broadly defined to include identification or association with a consumer or household, including demographics, usage, transactions and inquiries, preferences, inferences drawn to create a profile about a consumer, and education information, but excluding information from public government records used in a manner that is consistent with the government purpose, and also, it would appear, in some but possibly not all respects, de-identified data and aggregate consumer information (but this is unclear as the CCPA is currently worded). The definition of 'sell' is also broad, covering any 'selling, releasing, disclosing, dissemination, making available, transferring or otherwise communicating […] a consumer's personal information by the business to another business or a third party for monetary or other consideration.'

The CCPA limits incentives and penalties tied to the exercise of privacy rights

Under the CCPA, consumers have the right to equal service and price, meaning that a business cannot discriminate against a consumer because the consumer exercised any of the consumer's rights under the CCPA. However, a business can charge a consumer a different price or rate, or provide a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data. A business may offer financial incentives, including payments to consumers as compensation, for the collection of PI, the sale of PI, or the deletion of PI on an opt-in basis. A business that provides financial incentives must notify consumers of the financial incentives in accordance with the CCPA's requirements.

Penalties can be significant

A business can be assessed civil penalties of up to $2,500 per violation, or up to $7,500 for intentional violations, if the business is adjudicated liable in a civil action brought by the California Attorney General ('AG'), following a notice and failure to cure the violation within 30 days of the notice. The CCPA uses the AG's existing civil penalty authority for unfair business practices under §17206 of the California Business and Professions Code, but adds the potential of an increased penalty for intentional violations. The AG has in the past looked at conduct in a manner that enables it to calculate a number of violations that will result in a penalty it deems sufficient to punish illegal conduct so the potential aggregate liability could be significant. However, as noted below, since the CCPA has no express duty regarding data security, the potential penalty increase for intentional violations would not seem to be available for data security failures or breaches, but restricted to CCPA privacy violations.

There is also a narrow private right of action, but as passed, it is not applicable to violations of the CCPA, but rather, a consumer whose non-encrypted or non-redacted sensitive personal information, as defined under California's existing data security law[3], 'is subject to an unauthorised access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute' a private right of action for any of the following: (a) damages not less than $100 and not greater than $750 per consumer per incident, or actual damages, whichever is greater; (b) injunctive or declaratory relief; and (c) any other relief the court deems proper. Before initiating any action on an individual or class-wide basis, the consumer must provide the business 30 days' written notice identifying the specific provisions of the CCPA that the consumer alleges have been or are being violated, and a 30-day opportunity to cure, and a cure will preclude statutory damages. However, data security obligations are mandated under other California laws and not the CCPA, and since the consumer's CCPA cause of action is limited to data security failures following a breach, it is unclear what violation could be noticed or cured. Even if the duty of security is implied into the CCPA by the private right of action provision, it is not clear how a business could cure a past breach, or if prospectively curing the security inadequacies would be sufficient. This is one of the many examples of inartful drafting in the law as passed. Further, to be able to proceed, a consumer must give the AG notice within 30 days that the action has been filed, and the AG has the power to prohibit the private action from going forward. The CCPA limits private rights of action for CCPA violations to this narrow basis, as a 25 June amendment clarified that nothing in the act could be grounds for a private right of action under any other law, apparently intending to preclude having a violation of the CCPA serve as a basis for a claim under §17200 of the California Business and Professions Code that permits a private right of action for claims based on unlawful acts. However, the CCPA does not take away the private causes of action a 'customer' has under certain California data protection laws that predate the CCPA. Accordingly, some, but not all, data subjects may have causes of action following a security incident under multiples laws depending on whether they meet the differing definitions of consumer and customer.

Stay tuned for further changes

The CCPA was proposed as an alternative to an even stricter ballot initiative that was expected to appear on the November ballot and rushed into law as part of a compromise with the initiative's sponsor that resulted in the initiative being pulled. The CCPA is riddled with typos and has provisions that are vague or even fail to make sense, some of which are noted above. However, on 6 August 2018, SB 1121, an existing bill that had proposed another alternative privacy law that was passed over in favour of AB 375, was amended to propose amendments to the CCPA. So far, the proposed amendments are modest, mostly corrections of typographic errors and additions of some clarifying language. However, lobbyists and academics are working to try to expand the scope of the amendments. In addition to the potential for legislative amendment, the CCPA provides the AG with broad authority to promulgate regulations to 'further the interests' of the act, which could be another way to refine the CCPA and cure confusing provisions. Regardless of the likelihood of forthcoming modifications to the CCPA, businesses should assume that the finalised law will substantially increase the required level of privacy transparency and choice for consumers, and result in the need to revise data practices and implement data management systems, including vendor management, that will enable compliance.

Alan L. Friel Partner
afriel@bakerlaw.com
Niloufar Massachi Associate
nmassachi@bakerlaw.com
Baker Hostetler, Los Angeles

---

1. A ‘consumer’ is defined as a California resident, so employee data and other non-consumer data is covered.
2. The CCPA will regulate ‘businesses,’ defined as for-profit entities that have gross revenue in excess of $25 million; or that annually buy, receive for the business’ commercial purposes, sell, or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or, that derive 50 percent or more of its annual revenues from the sale of consumers’ personal information, as well the similarly branded affiliates of such an entity
It should be noted that over the course of a year it will not take much to reach the 50,000 data points threshold – e.g., an average of 138 credit card transactions or unique web site visits per day would suffice.
3. §1798.81.5(d)(1)(A) of the California Civil Code (first name or initial with last name plus other data such as ID or account number, but not PI as defined under §17981.5(d)(1)(B) involving username or address plus a password or security question).