BakerHostetler

Overview of the New California Consumer Privacy Law

In late June, California enacted Assembly Bill 375 (AB 375) as the California Consumer Privacy Act of 2018 (CCPA), a privacy law, unprecedented in the U.S., that grants California residents a broad range of European-like rights when it comes to their personal information (PI), effective Jan. 1, 2020. AB 375 was passed as part of a compromise with a sponsors of a consumer privacy ballot initiative that resulted in keeping the initiative off of the November ballot. To be able to comply on the effective date, businesses will need to start record-keeping no later than Jan. 1, 2019, and likely will need to complete data mapping prior to that. Data inventorying and management vendors are scrambling to update their platforms to enable businesses to do so, and the cost of such solutions is projected to be significant – estimated at $50,000 to $100,000 a year. Given that processing an average of 138 credit cards a day, or having an average of 138 unique website visits a day, or a combination thereof and other data collection, is enough to draw a business under the scope of the law, all but the smallest businesses will need to comply. There are also certain obligations and liabilities for certain types of service providers processing the data of a regulated business, and other third parties.

The California attorney general's office (CaAG or attorney general), which has exclusive authority to enforce the CCPA (excepting a narrow private right of action for data security breaches that overlaps other existing California laws), may give businesses and service providers some leeway in becoming fully compliant by the effective date. Indeed, it will take time for the CaAG to promulgate the regulations that will guide compliance. However, the legislative history of AB 375 indicates that the CaAG estimates it will need 57 full-time staff to enforce the CCPA and that it will need to secure over $57.5 million in civil penalties to cover that cost, suggesting that enforcement may be robust. However, before the CaAG can seek penalties, it must give businesses notice and a 30-day opportunity to cure, which likely will enable businesses that are mostly in compliance to avoid enforcement actions if they have already done most of the legwork that will enable them to quickly remediate inadequacies.

Further, the bill's sponsor and other legislators have stated that they plan to further refine the law through amendments, and on Aug. 6, 2018, SB 1121 (which had proposed various changes to California's data privacy and security laws that predate the CCPA) was amended to make revisions to the CCPA. SB 1121 passed on Aug. 31, 2018, and is currently awaiting action by Gov. Brown, who has until Sept. 30 to sign the bill. If the bill is signed, the amendments would, among other things, extend the time for the CaAG to promulgate regulations until July 1, 2020, and stay enforcement by the CaAG until the later of July 1, 2020, or six months from issuance of the regulations. There will likely be ongoing legislative efforts in the coming months to refine the CCPA, but the initiative's sponsors have pledged to revive the ballot initiative if the CCPA is amended in a way that is inconsistent with the compromise that AB 375 reflects. Prudent companies will become familiar now with what the law will require and start to work with their legal and IT departments on compliance.

In short, all Californians (the law governs PI of "consumers," defined as California residents, so employee data and other nonconsumer data are covered) will have the right to demand that a covered business provide them with a transportable copy of their PI, delete their PI, not sell their PI, and provide them with both generic and consumer-specific information about PI collection and sharing. The CCPA will regulate "businesses," defined as for-profit entities doing business in California (or with Californians not in all respects outside of California) that are the controllers of the data and that have gross revenue in excess of $25 million; or that annually buy, receive for the business's 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 their annual revenues from the sale of consumers' personal information. The 50,000 threshold will be quickly met by companies that accept credit cards and/or run websites, as each unique card collected and site visitor IP address will count toward that number, which works out to be an average of 138 such data points a day. Also covered is any affiliate of any such entity that operates under the same brand.

Specifically, regulated businesses (and in some circumstances other parties such as certain types of service providers of a regulated business, parties that are sold PI and successors in interest to a covered business) will need to prepare to comply with the CCPA. Examples of what will be required by the CCPA include:

- A business must track PI collected; inform consumers, at or before collection, of the categories of PI collected and the purposes (business and commercial) for the collection of each category; and limit the use to those purposes absent further advance notice.
- A business must inform consumers of the following, in a form readily accessible to them:
  - A description of consumers' rights under the CCPA, which shall be in the business's online privacy policy (if any) and any California-specific privacy notices.
  - A link to the business's "Do Not Sell My Personal Information" web-based opt-out tool, both on its internet home page and in its online privacy policy (if any) and any California-specific privacy notices.
  - Two or more designated methods for submitting information requests, including at minimum a toll-free number and a website address if the business has a website, excepting that in any online privacy notices only one additional method beyond the website method need be listed.
- Further, a business must inform consumers in any online privacy policies and any specific privacy notices to California residents, or otherwise on the business's website, of:
  - Consumers' rights under the CCPA.
  - A list of categories of PI (11 specific categories of PI are to be used) collected in the preceding 12 months and the purposes (business and commercial) therefore; use for any other purpose requires further notice prior to different use.
  - 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 inform the consumer of that fact).
  - 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 state that). While there is no obligation to include a list of categories of PI disclosed for a commercial purpose in the preceding 12 months, it is recommended that both purposes be included in such policies or notices, and that the purposes be distinguished. The distinction between the two categories is whether the purposes are merely operational (business) or also to advance an economic interest, such as for marketing (commercial).
  - The CCPA is internally inconsistent as to whether the online notice needs to include the categories of sources from which PI is collected, the categories of third parties with which PI is shared and the specific pieces of PI collected about a specific consumer. Compare CA Civil Code §1798.130(a)(5) with §1798.115(c)(2), (4) and (5). Obviously, the last requirement could not be accomplished in a general notice. However, it is recommended that the other information be included in the online notice.
  - Any consent-related incentives.
- Upon a verified request from the consumer, a business must provide the following information to the consumer on an individualized 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 purpose(s) and commercial purpose(s) for collecting or selling the PI.
  - The categories of third parties (which includes differently branded affiliates, and possibly similarly branded affiliates, but does not include service providers engaged for business purposes if certain requirements are met, but does include vendors for commercial purposes) 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 (likely including affiliates).
  - For PI that is disclosed for a business purpose, the categories of the consumer's PI that were disclosed. There is no obligation to include in a request response the categories of PI disclosed for commercial purposes, though that may be added before the effective date, and it is suggested that this also be provided.
- In addition, the CCPA requires that:
  - Any party that is sold PI, even if not a regulated business, may not resell it without first giving the consumer notice of the right to opt out of sales and must accept and honor opt-outs.

- Businesses that have collected PI and sell it, and parties that sell PI even if not otherwise a covered business, must:
  - Have a clear and conspicuous link on their internet homepage titled "Do Not Sell My Personal Information" that goes to an opt-out mechanism.
  - Include a "Do Not Sell My Personal Information" notice in their online privacy notices/policies that links to the opt-out mechanism.
  - Be able to cease selling PI upon request, and must not solicit opt-in for 12 months following an opt-out.
  - Obtain from youths under 16 opt-in consent to sell PI, which consent must be from the parent or guardian if the consumer is under 13.
- The data deletion, portability and information rights of the CCPA appear to apply only to a covered business and do not currently seem to apply to a party that is sold PI by a business but is not itself a business.
- In order to be able to modify data so that it is not restricted by the act's collection, use, retention, sale and disclosure requirements, a business may de-identify PI so that it "cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses de-identified information" has implemented technical and business process safeguards to prevent and prohibit re-identification and to avoid inadvertent release of de-identified information, and makes no attempts to re-identify.
- Vendor agreements will need to provide for a service provider to restrict or delete consumer information on request and for the business to keep track of what service providers have what PI so that it can make such requests when a consumer has made a deletion demand. Due to the definition of "service provider," this currently applies only to certain vendors engaged for narrow business purposes, but not to those engaged for commercial purposes (e.g., marketing and sales) who are defined as third parties rather than service providers.
- A recipient of PI as part of a permitted corporate transaction (e.g., merger or sale) may not alter how it uses or shares PI from the ways represented by the original business at the time of collection without first giving the consumers notice of the new or changed practices.

The right to individualized 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. Again, since the required look-back period is 12 months, businesses should start maintaining this information as of Jan. 2019 to be able to comply with requests made shortly after the law goes into effect as of Jan. 2020. A business must respond to a consumer's verified request for information within 45 days, subject to extension under limited circumstances. Further, as noted above, it must provide at least two methods for submitting requests for information, which must include 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 under ordinary circumstances, charge the consumer, as a condition of fulfilling a request.

In addition to accommodating consumers' information rights, 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 a portable and, to the extent feasible, a readily usable format that allows the consumer to transmit the PI to another entity without hindrance, and to delete PI upon request (including causing the business's service providers to also delete such PI). Businesses are not required to provide PI, or the required details on PI practices, to a consumer more than twice in a 12-month period. However, there appears to be no limit on data deletion requests. 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.

The CCPA Treats Personal Information and Its Collection and 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 data *capable of* identification of *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, and potentially also de-identified data and aggregate consumer information (but this is far from clear as the bill 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." Similarly, the definition of "collection" is also very broad – "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a customer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior."

The CCPA Limits Incentives and Penalties Tied to 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 on an opt-in basis, including payments to consumers as compensation, for the collection of personal information, for the sale of personal information or regarding deletion of personal information. 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 CaAG following a notice and failure to cure the violation within 30 days of notice. The attorney general's office 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 increased per-violation penalty for intentional violations would not seem to be available for data security failures or breaches, but be 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 to where a consumer whose nonencrypted or nonredacted first name or initial with last name plus other data such as ID or account number "is subject to an unauthorized 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." In such case, the consumer may initiate 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 classwide basis, the consumer must provide the business written notice identifying the specific provisions of the CCPA that the consumer alleges have been or are being violated, and provide a 30-day opportunity to cure. A timely cure will preclude statutory damages. However, data security obligations are mandated under other California law and not the CCPA, and the consumer's CCPA cause of action is limited to data security failures following a breach, so it is unclear what violation could be noticed or cured. Even if the duty of security is implied in the CCPA by the private right of action provision, it is not clear how a business could cure a past breach or whether 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 attorney general notice within 30 days that the action has been filed, and the attorney general has the power to prohibit the private action from going forward. SB 1121, however, will eliminate the CaAG notice and ability to intervene if the bill becomes law. The CCPA limits private rights of action for CCPA violations to this narrow basis, as a June 25 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 act serve as a basis for a claim under California Business and Professions Code Section 17200, which permits a private right of action for claims based on unlawful acts. There is, however, no express statement of that intent in the Act or its legislative history, and plaintiffs' lawyers may challenge the effectiveness of this language to bar 17200 claims. Further, the CCPA

does not preclude the pre-existing right under other California law of "customers" to bring suit for injuries incurred by a data security breach. This results in the potential for data subjects that are both "consumers" and "customers" to have two different potential private rights of action following a security incident.

Expect Refinements but Start Addressing the Principles

AB 375 was proposed as an alternative to an even stricter ballot initiative that was expected to appear on the November ballot, and was rushed into law as part of a compromise with the initiative's sponsor that resulted in the initiative being pulled. While watering down the private right of action and making other changes desired by industry, the legislature added several European-inspired provisions such as the consumer-specific information rights, data portability and deletion rights. The legislative history specifically references the European Union's General Data Protection Regulation (GDPR), which became effective in May and states: "California consumers should similarly be able to exercise control over their personal information, and should have reasonable certainty that there are safeguards in place to protect against the misuse of their personal information." While businesses that have already become GDPR-compliant will have a head start over those that have not, because they will have completed data mapping and implemented data inventory and processor management tools and programs, there are sufficient material differences between the two schemes that even GDPR-compliant companies will have work to do to prepare for CCPA.

The CCPA is riddled with typos and has provisions that are vague or simply do not make sense, some of which are noted above. As noted, SB 1121 has been passed and is awaiting action by the governor, and if passed would make some changes and potentially delay enforcement. However, the legislature remains under threat of a revived ballot initiative if it substantively waters down the law, so the CCPA's key requirements are not expected to change beyond refinement that is consistent with the overall intent of the law as already passed. In addition to the potential for legislative amendment, the CCPA provides the CaAG 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 finalized law will substantially increase the required level of privacy transparency and choice for consumers, and result in the need to implement data management systems and practices that will enable compliance. Further, given the 12-month look-back for responding to consumer requests, businesses should start doing so in Jan. 2019 in order to be ready to respond to consumer demands come Jan. 1, 2020.

Contacts

Janine Anthony Bowen
jbowen@bakerlaw.com
T +1.404.946.9816

M. Scott Koller
mskoller@bakerlaw.com
T +1.310.979.8427

Alan L. Friel
afriel@bakerlaw.com
T +1.310.442.8860

Melinda L. McLellan
mmclellan@bakerlaw.com
T +1.212.589.4679

Laura E. Jehl
ljehl@bakerlaw.com
T +1 202.861.1588

21.09.18.12.37_p00