Preparing for California's New Privacy Law Will Make for a Busy 2019 for Legal, IT and Info Governance Departments

BY

Alan Friel
BakerHostetler

Overview of the CCPA

California has enacted, effective Jan. 1, 2020, the California Consumer Privacy Act (CCPA), a privacy law unprecedented in the U.S. that will create significant compliance challenges for media and entertainment companies. The CCPA grants California residents (referred to as “consumers” in the act but not limited to consumers) a broad range of European-like privacy rights in regard to their personal information (PI), broadly defined. To enable compliance with the act, covered businesses will be required to implement data management practices that increase consumers' transparency and choice. For example, the CCPA requires that a business that falls under the act must track PI collected, shared and sold (also broadly defined) and inform consumers of certain details of such activity both in general privacy notices and on a consumer-specific basis in response to a qualifying request. In addition, to comply with the CCPA, a business must provide access to and portability of a consumer's PI and, subject to certain exceptions, delete consumer PI upon request. Further, a business is required to inform consumers of their rights under the CCPA, and have and honor a “Do Not Sell My Personal Information” web-based opt-out tool and program that enable consumers to prevent the sale of their PI.

Amendments to the CCPA

The California Legislature amended the CCPA on Aug. 31 by passing SB-1121, which the governor signed. The legislature was expected to amend the CCPA, which passed just about one week after it was proposed, in a rush in order to avoid a different version of the act being finalized as a ballot initiative on the November ballot. The amendments extend the time to July 1, 2020, for the California attorney general (CaAG) to promulgate regulations, push back enforcement until the earlier of that date or six months from issuance of the regulations, and remove the CaAG's ability to intervene in private lawsuits - changes made at the request of the CaAG. Fortunately for businesses, the CaAG's recommendation that the CCPA's limited private right of action be expanded was rejected, and language was even added to SB-
1121 to clarify the limits of consumer lawsuits. Unfortunately, the CaAG has indicated that he expects to have final regulations out by June 2019, so do not count on the potential enforcement delay. Also, be aware that consumer information requests have a 12-month look back, so when the law becomes effective on January 1, 2020, a business will need to be able to respond with customer-specific data information as of January 1, 2019. Most companies will need to make significant data management changes to be able to do so and thus need to begin that process now.

While SB-1121 did make needed changes to the CCPA, many more issues need to be addressed. Chief among these are the need to harmonize the CCPA, which is Title 1.81.5, with existing Title 1.81. The legislature should amend Title 1.81 to do away with the existing private right of action for "customers" under Title 1.81 and have the new private right of action under Title 1.81.5 for consumers be the exclusive private right of action for data security failures. Moreover, it should repeal altogether the Shine the Light Act in Title 1.81, which regulates sharing of customers' PI for third-party marketing now that the CCPA's more comprehensive consumer privacy rules are in place, or it should at least sunset the Shine the Light Act when the CCPA becomes effective. Otherwise, covered businesses will struggle with two different but overlapping California transparency and choice regimes - including the need to post home page links on their websites to both Your California Privacy Rights for notice of Shine the Light Act rights along with a Do Not Sell My Personal Information link for notice of CCPA opt out. For a more detailed discussion on conflicts and problems with the act, see Professor Eric Goldman's blog post here.

Preparing for the CCPA

The U.S. Chamber of Commerce is lobbying Congress to pass a federal omnibus privacy and data protection law that would pre-empt the CCPA and other existing and future state data protection laws. Assuming no federal pre-emption, businesses need to begin to prepare for the CCPA. As noted, to comply with the 12-month look back for consumer requests as of the law's effective date, businesses will need to start data-mapping and record-keeping of PI as of Jan. 1, 2019. 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 - $50,000 to $100,000 or more a year.

Under the CCPA, all Californians (the law governs PI of consumers, defined as California residents, so employee data and other non-consumer 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 (subject to some retention exceptions), 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 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' commercial purposes, or sell or share for commercial purposes the PI of 50,000 or more consumers, households or devices; or that derive 50 percent or more of their annual revenue from the sale of PI. The 50,000 threshold will be quickly met by brands 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. There are also obligations and liabilities for certain types of service providers processing data of a regulated business and for other third parties. There is a broad exemption for covered entities and business associates under the federal and California healthcare privacy laws, and there is an exclusion of PI collected, processed, sold or disclosed pursuant to federal and California laws regulating financial institutions.

A business must track PI collected and inform consumers at or before collection and in any online privacy policy of the categories of PI collected (11 specific categories of PI are to be used) and the purposes (business purposes or commercial purposes, defined differently) for the collection of each category; it must also limit the use for those purposes absent further advance notice. A business must also inform consumers of certain of its PI collection, sharing and sales practices in its privacy policy; inform consumers of their rights under the CCPA in accordance with the act; and have and honor a Do Not Sell
My Personal Information web-based opt-out tool and program that enable consumers to prevent the sale of their PI. 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. A business must not solicit an opt in for 12 months following an opt out, and opt-in consent required if the youth is under 16. There must be two or more methods for submitting information requests, which must include at least a toll-free number and a website address (if the business has a site).

The types of information to which a consumer is entitled upon request are detailed and are on a customer-specific basis, though not on a recipient-specific basis. A business cannot require the consumer to create an account or under ordinary circumstances charge the consumer as a condition of fulfilling a request. 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.

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. 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 PI or the sale of PI or regarding deletion of PI. A business that provides financial incentives must notify consumers of the financial incentives in accordance with the CCPA's requirements.

A recipient of PI as part of a merger or asset 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 consumer notice of the new or changed practices, and the recipient in a sale of data cannot resell the PI without notice and an opportunity for the consumer to opt out.

A business must promptly disclose and deliver a copy of a consumer's PI, if requested, in a readily usable format that allows the consumer to transmit the PI to another entity without hindrance, and it must delete PI upon request (including causing the business’ service providers to also delete such PI). In particular, a business must respond to a consumer's verified request for information within 45 days, subject to extension under limited circumstances. 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.
A business can be assessed civil penalties of up to $7,500 per violation in a civil action brought by the CaAG following a notice and failure to cure the violation within 30 days of notice. There is a narrow private right of action, but it is applicable only to certain data breaches where the business failed to maintain reasonable security procedures and practices, and not to privacy violations. The August amendments made this limitation even more clear. Consumers 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.

The act includes language that should serve to preclude using a violation of CCPA as the basis for a claim under other consumer protection laws, though the class action bar may challenge that. The bill that became the CCPA was amended on June 25 to add subsection (c) of Section 1798.150 to clarify "Nothing in this act [now 'title'] shall be interpreted to serve as the basis for a private right of action under any other law." Based on this language, it appears that the California Legislature intended to preclude having a business' violation of the CCPA serve as a basis for a claim under California's Unfair Competition Law (UCL), California Business and Professions Code (BPC) §§ 17200 et seq., which permits a private right of action for claims based on unlawful, unfair or fraudulent business acts or practices - or under "any other law." The Electronic Frontier Foundation (EFF) reads the act the same way, as it has urged the Legislature to amend it to allow for a broader private right of action. In particular, the EFF has stated, "Unfortunately, the private right of action in the CCPA is woefully inadequate. It may only be brought to remedy certain data breaches. See Section 150(a)(1). The Act does not empower users to sue businesses that sell their data without consent, that refuse to comply with right-to-know requests, and that refuse to comply with data portability requests. EFF urges the California legislature to expand the Act's private cause of action to cover violations of these privacy rights, too." See https://www.eff.org/deeplinks/2018/08/how-improve-california-consumer-privacy-act-2018.

California's attorney general, Xavier Becerra, has also urged expansion of the private right of action. In a letter he wrote to the California State Assembly and the California State Senate on Aug. 22, 2018, he stated, "[T]he CCPA does not include a private right of action that would allow consumers to seek legal remedies for themselves to protect their privacy. Instead, the Act includes a provision that gives consumers a limited right to sue if they become a victim of a data breach." In his letter, the attorney general urges the Legislature to provide consumers with a private right of action under the CCPA.

As with so much else of the CCPA, the Legislature's intent to preclude CCPA violations from being the basis for a UCL claim could be better expressed in the act, and the official legislative history is sparse. In New York Times Magazine's reporting on the negotiations between the supporters of the consumer privacy ballot initiative, who pulled their initiative in exchange for the passage of the CCPA, and industry, which was mediated by the CCPA's authors, it appears that the intent was to preclude any private cause of action whatsoever arising out of the privacy provisions of the CCPA. Notwithstanding the June 25 amendment prohibiting use of a violation of the CCPA to "serve as the basis for a private right of action under any other law," plaintiffs may attempt to use the CCPA as a legal predicate for alleged violations of the "unlawful" prong of the UCL. BPC §§ 17200 et seq. The UCL itself provides for a private right of action and simply borrows from other state and federal laws in determining what can constitute "unlawful" activity. Existing case law holds that a statute can be used as the legal predicate for a violation of the UCL even if it does not itself provide for a private right of action, unless there is express legislative intent to the contrary. So the question facing the courts will be whether "[n]othing in this act [or title] shall be interpreted to serve as the basis for a private right of action under any other law" provides the express legislative intent necessary to prevent UCL claims based on alleged violations of the CCPA. The language suggests a legislative intent to disallow the CCPA to be used as the legal predicate for a UCL claim, but the lack of specificity invites litigation over how clearly that intent has been expressed. The question could be put to rest if the legislature were to reword the provision to say something like "Nothing in this Title 1.81.5 shall be interpreted to serve as a basis for a private right of action under any other law, and specifically there shall be no private cause of action to recover remedies available under Business
and Profession Code §§ 17200 et seq., or other similar consumer protection laws as a result of a violation of this Act.” The Legislature should clarify its intent now, while it is already trying to clarify the limits of the private right of action under Section 1798.150.

**Conclusion**

While businesses that are compliant with the European General Data Protection Regulation (GDPR) will have a head start on those that are not - because they will have completed data-mapping and implemented data inventory and processor management tools and programs - there are material differences between the two schemes such that even GDPR-compliant companies will have work to do to prepare for CCPA. And for those businesses that missed the GDPR bullet, absent an act of Congress that pre-empts the CCPA, the time has come to develop robust data management. Regardless of whether the Legislature further amends the CCPA, businesses should assume that the finalized CCPA will substantially increase the required level of privacy transparency and choice for consumers, and it will result in the need to implement data management systems and practices that will enable compliance. To do so, businesses should start developing more robust data management in early 2019 in order to be ready to respond to consumer demands come Jan. 1, 2020. AMEC is co-sponsoring a program that will outline how to prepare for the CCPA at 8 a.m. on November 16, 2018, as part of UCLA’s Big Data Conference. Admission is free for AMEC members, who may also attend the main conference at a discount. For more information and to register, click here.

**About The Author**

Alan Friel is a partner in the advertising, marketing & digital media and privacy & data protection groups of BakerHostetler, resident in the Los Angeles and Orange County offices. He advises leading companies on privacy and data protection and digital media and advertising issues. He is a Certified Information Privacy Manager by the International Association of Privacy Professionals and has led hundreds of privacy impact assessments and data protection compliance projects. He is currently assisting dozens of companies with developing and implementing 2019 CCPA compliance project plans.