CORPORATE COUNSEL
An ALM Website
corpcounsel.com | December 10, 2018

A Practical Guide to CCPA Readiness: Implementing Calif.'s New Privacy Law (Part 1)

By Harry A. Valetk and Brian Hengesbaugh

California is a remarkable jurisdiction by any measure. It has the largest economy in the United States, represents the third largest state in the United States in terms of total area at 163,696 square miles, and stands as the fifth largest economy in the world with a gross domestic product at more than $2.7 trillion. And, now, thanks to its recently enacted California Consumer Privacy Act of 2018 (CCPA), it also has the most far-reaching privacy law in the United States.

CCPA is an unfamiliar type of law for the United States due, in large part, to its broad scope. It establishes a new privacy framework for businesses that fall within its jurisdiction by:

- Creating an expanded definition of "personal information";
- Creating new data privacy rights for California consumers, including rights to know, access, delete, and opt out of the "sale" of their personal information;
- Imposing special rules for the collection and sale of personal information directly from minors; and
- Creating a new statutory damages framework for violators that fail to implement and maintain reasonable security procedures and practices to prevent data security breaches.

As a result, CCPA has significant implications for almost every commercial enterprise. But it is important to reach a firm understanding on the law's scope, key terms, and exceptions before deciding on an plan of action for implementation.

In an effort to help companies organize how to prepare for CCPA readiness, we prepared a two-part series describing various legal and operational steps for organizations to consider when implementing CCPA's requirements. In this first part, we outline CCPA's scope and potential retroactive provisions. We ask and answer three important questions:

1. **Does CCPA apply to me?**
2. **What are the exceptions to CCPA?**
3. **When will CCPA go into effect?**

Does CCPA Apply to Me?

The first important question to answer is whether CCPA applies to your organization. CCPA only applies to organizations that conduct business in California, and satisfy one of the following three conditions:

- Has annual gross revenue in excess of $25 million;
- Annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices, alone or in combination; or
- Derives 50 percent or more of its annual revenue from selling consumers' personal information (each, a covered business).

CCPA also applies to any entity that "controls or is controlled by" any covered business.

CCPA applies to the sale of personal information. "Sale" is a broad term defined as, "the selling, renting, releasing, disclosing, disseminating, 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 valuable consideration." The following circumstances, however, do not constitute sale of personal information:

- Consumer-directed disclosure or use that was intended by the consumer;
- Use of personal information for the purposes of identifying a consumer who has opted out under the opt-out provision;
- Sharing personal information with a service provider that is necessary for the performance of a business purpose, if the business has provided notice to its consumers, the service provider is acting on the business's behalf, and the service provider does not sell the personal information; and finally,
- The business transfers Personal Information to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction where the third party "assumes control of all or part of the business," subject to certain condition

What is personal information? CCPA applies to all personal information collected by a covered business from consumers. "Consumers" means any natural person who is a California resident. Personal information is broadly defined to mean "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." CCPA excludes "aggregate consumer information" from the definition of personal information. "Aggregate consumer information" means data that is, "not linked or reasonably linkable to any consumer or household, including via a device." Also, information that is publicly available from federal, state, or local government records is similarly excluded.

What Are the Exceptions to the Law?

CCPA creates several exceptions. By its terms, CCPA will not restrict a business's ability to:

- Comply with federal, state, or local laws.
- Comply with civil, criminal, or regulatory inquiries or investigations.
- Cooperate with law enforcement agencies.
- Exercise or defend legal claims.
- Collect, use, retain, sell or disclose consumer information that is "de-identified" or "aggregate consumer information." "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed and is not reasonably likable to a consumer or device. "Deidentified" means information

that, "cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer." To fall within this exception, businesses must implement technical safeguards that prohibit re-identification, business processes that specifically prohibit re-identification, business processes to prevent inadvertent release of de-identified information, and finally, they must make no attempt to re-identify information.

• Collect or sell consumer information so long as every aspect of the commercial conduct takes place outside of California—meaning that the data was collected while the consumer was outside the state and no part of the sale occurred within the state.

CCPA also does not apply where:

• Compliance would interfere with or violate evidentiary privileges;

• The information is medical information governed by the Confidentiality of Medical Information Act or protected health information governed by the Health Insurance Portability and Accountability Act of 1996;

• The sale of information is to or from a consumer reporting agency that is to be reported in or used to generate a consumer report;

• The information is collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act (Public Law 106–102) or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code); and finally,

• The information is collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721 et seq.).

Based on the above, it is important for covered businesses to perform appropriate internal diligence to determine if an exception applies, and to what extent. Doing so will likely help refine the scope and cost of implementation and solidify overall readiness efforts.

When Will CCPA Go Into Effect?

CCPA is set to become effective on Jan. 1, 2019, but "operative" on Jan. 1, 2020, unless it is amended by the state of California, or preempted by federal privacy law. CCPA also directs the California Attorney General to adopt regulations on various provisions within CCPA. The Attorney General may not bring an enforcement action under CCPA until six months after adoption of those regulations, or July 1, 2020, whichever is sooner.

In our next article, we will discuss specific steps companies should take to achieve CCPA readiness. There is little doubt that we are in the midst of a regulatory transformation in data use, and in-house counsel must continue to strategically assess the privacy and security risks associated with collecting, using, and sharing personal information, and manage the business expectations in light of the regulatory enforcement trends.

Harry A. Valetk *is a member of Baker McKenzie's global privacy and security practice group based in New York, where he focuses on advising clients on global privacy compliance and cyber security practices. He can be reached at harry.valetk@bakermckenzie.com.*

Brian Hengesbaugh *is a partner and chair of the firm's global privacy and security practice group based in Chicago. He focuses on global data privacy and data security issues in business transformations, compliance activities, and incident response/ regulatory inquiries. He can be reached at brian.hengesbaugh@bakermckenzie.com.*

Baker McKenzie.

CORPORATE COUNSEL
An ALM Website
corpcounsel.com | December 18, 2018

A Practical Guide to CCPA Readiness: Implementing Calif.'s New Privacy Law (Part 2)

By Harry A. Valetk and Brian Hengesbaugh

This is the second article in a two-part series discussing readiness steps organizations should consider when implementing the California Consumer Privacy Act of 2018 (CCPA). As we previously discussed, CCPA establishes a new privacy framework for "covered businesses" that fall within its jurisdiction by:

- Creating an expanded definition of "personal information";
- Creating new data privacy rights for California consumers, including rights to know, access, delete, and opt out of the "sale" of their personal information;
- Imposing special rules for the collection and sale of personal information directly from minors; and
- Creating a new statutory damages framework for violators that fail to implement and maintain reasonable security procedures and practices to prevent data security breaches.

A "covered business" refers to businesses described in Cal. Civ. Code Section 1798.140(c).

Accordingly, businesses must understand the impact CCPA will have on operations, what exceptions may apply, and how to organize readiness activities. In this second part, we outline eight specific steps toward CCPA readiness.

1. **Establish and maintain a data inventory of personal information collected or sold from California residents.**

Perform review of IT systems to document the categories of personal information.

- Collected from California residents in the past 12 months; and
- Sold—or disclosed for business purposes—in the past 12 months.

Another key feature of this workstream is to understand what policies, procedures, notices, agreements and other relevant documentation are already in place to avoid duplicating efforts. In fact, performing this work in earnest will help shape future readiness activities. Some businesses may have the internal resources and expertise to conduct this review in-house, while others may need to retain external consultants to perform a reliable assessment and identify data in-scope for CCPA (including legacy systems and unstructured data).

In addition, understanding data inventories could help determine if your business falls within CCPA's scope because you buy, receive, sell or share personal information of 50,000 consumers or more.

2. **Revise and update privacy notices (Section 1798.100(b) and 1798.130(a)(5))**

Organizations subject to CCPA must also affirmatively disclose the following in their online privacy policy:

- At or before the time of collection, what personal information it will collect about consumers and the

purposes for which that data will be used;
- A description of a consumer's rights and one or more designated methods for submitting requests;
- The categories of consumer personal information that were actually collected in the preceding 12 months; and
- The categories of consumer personal information that were sold or disclosed for "business purposes" in the preceding 12 months.

Note that these categories of personal information must be disclosed by reference to the enumerated categories in Section 1798.110(c). For example, Section 1798.110(c)(3) of CCPA requires covered businesses to disclose—not only what personal information was collected—but also information about, "the business commercial purpose for collecting or selling personal information."

As part of this exercise, covered businesses will also need to decide if they wish to maintain one privacy notice for California residents and one for other consumers, or just have one universal policy.

3. **Verifiable consumer requests.** CCPA requires covered businesses to respond within 45 days from receipt of a verifiable consumer request with specific and accurate disclosures about:

• What categories of the requesting consumer's personal information were actually collected in the past 12 months.

• What categories of the requesting consumer's personal Information were sold or disclosed for business purposes in the past 12 months.

Data collection. CCPA also requires that covered businesses responding to verifiable consumer requests about data collection include information about:

• The categories of sources from which personal information was collected;

• The business or commercial purpose for collecting or selling that personal information;

• The categories of third parties with whom the business has shared personal information; and

• The specific pieces of personal information it has collected about that consumer.

Selling or disclosures. For responding to verifiable consumer requests about data sales or disclosures, covered businesses must disclose, as applicable:

• The categories of personal information sold and to whom it was sold; or

• The categories of personal information disclosed for a business purpose and to whom it was disclosed.

Contacting covered businesses. Covered businesses must also provide at least two methods by which consumers may make verifiable consumer requests for disclosures. At a minimum, this includes:

• Toll-free number; and

• Online form.

Authentication and secure transmission. Business IT systems must be able to authenticate each consumer before responding directly to specific requests. Any personal information transmitted to a verified consumer should be sent securely and encrypted in-transit.

If a covered business does not collect sufficient personal information to verify or otherwise authenticate the identify of the consumer, then it may not require that consumer to create an account or supplement information to verify the request. Covered businesses in this situation may be unable to respond to consumer requests for information.

4. **Access rights (Section 1798.110(a)(5)).** CCPA guarantees consumers the right to access a copy of the "specific pieces of personal information that [a business] has collected about that consumer" to be delivered either by mail or electronically.

• IT systems must be capable of identifying personal information provided to the covered business directly by the consumer, and compiling that personal information in a portable and, to the extent technically feasible, in a readily useable format to be provided to a consumer or third party.

• All the time, covered businesses must be able to securely authenticate the consumer. In cases where a covered business is processing personal information on behalf of another business, however, those IT systems must be capable of assisting corporate customers directly subject to CCPA to comply with this requirement.

• **Data Retention.** IT systems must be able to retain personal information to respond to verifiable access requests (likely 12 months or as otherwise required by applicable law). Covered businesses should also develop policies for the secure disposal of personal information no longer needed for legal or business reasons.

5. **Erasure rights (Section 1798.105).** CCPA empowers consumers to request the deletion of their personal information from business servers and service providers. Covered businesses must be prepared to honor the deletion request, unless an exception applies. Those exceptions include situations where it is necessary to maintain the personal information to:

• Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or otherwise perform a contract between the business and the consumer.

• Detect and maintain data security.

• Debug to identify and repair errors.

• Exercise a right provided for by law.

• Comply with the California Electronic Communications Privacy Act.

• Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest when deletion would render it impossible or seriously impair the achievement of such research.

• Comply with legal obligations.

• Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

• Otherwise use the consumer's personal information internally in a lawful manner that is compatible with the context in which the personal information was provided.

In cases where the covered business is acting as a data processor, IT Systems must be capable of assisting corporate customers to comply with this erasure requirement.

6. **Right to opt-out of sale of personal information (Section 1798.120).** CCPA gives consumers the right to opt-out of the sale of their personal information to third parties. If an individual consumer does not affirmatively opt out, then their data may be sold without further action (provided that sale is disclosed in the business's privacy policy). To comply, covered businesses must:

- Post a "clear and conspicuous" link titled "Do Not Sell My Personal Information" on website.
- Describe the right and include a link to the opt-out page in privacy policy.
- Ensure individuals responsible for handling consumer inquiries are trained about opt-out requirements and how to direct consumers to exercise their opt-out rights.

In addition, IT systems must be able to:

- Authenticate each consumer before responding directly to specific requests.
- Honor "Do Not Sell" requests
- Refrain from re-asking consumer for consent to sell "for at least 12 months before requesting that the consumer authorize the sale of" their personal information.
- Process opt-out requests from authorized representatives.

Restrictions on sale of minors' personal information. CCPA also affords minors special protections. Specifically, CCPA generally prohibits the sale of personal information if the business has actual knowledge that the consumer is under 16 years of age or willfully disregards the consumer's age. To sell that data, covered businesses must:

- Ages 13 through 16: obtain affirmative consent to sell personal information directly from consumer.
- Ages 0 through 13: obtain parental consent to sell personal information.

In addition, IT systems must be able to:

- Authenticate each consumer before responding directly to specific requests.
- Treat consumers differently depending on the consumer's age.
- Identify, adequately inform, and obtain appropriate or verified parental consent securely to sell a minor's personal information.
- Retain consent for as long as covered business maintains relationship with consumer.

7. **Update service level agreements with third-party data processors.** Covered businesses should assess contractual commitments with third party data processors:

- Assess the categories of personal information processed by third parties.
- Assess whether processing activities meet the definition of "selling" under CCPA, or if a statutory exception applies.
- Explore the possibility of re-negotiating those arrangements to avoid the definition of "selling."

8. **Covered businesses must also train personnel with access to personal information about CCPA requirements.** CCPA mandates that individuals responsible for handling consumer inquiries or the Covered business' compliance be "informed" of relevant statutory requirements.

- Develop CCPA awareness training for in-scope personnel.
- Monitor authorized users of IT systems containing personal information, including those belonging to minors.
- Written procedures, guidelines, and standards to ensure the use of CCPA-compliant development practices for in-house IT applications.
- Procedures to evaluate compliance of externally developed IT applications.
- Maintain current knowledge of CCPA legislative developments, including guidance from Attorney General.
- Due diligence and onboarding process for third party service providers' compliance with CCPA requirements.
- Periodic assessment of third party IT systems.
- Representations and warranties about third party service providers' compliance with CCPA.

Stay tuned on additional legislative developments related to CCPA that are sure to come, as the California's Attorney General must still also adopt implementing regulations—after broad public participation—no later than July 1, 2020. Beyond that, it is important to bear in mind that various industry groups are still advocating for legislative clarifications, so additional changes may occur before this law goes into full effect in 2020.

Harry A. Valetk *is a member of Baker McKenzie's global privacy and security practice group based in New York, where he focuses his practice on advising clients on global privacy compliance and cybersecurity practices. He can be reached at harry.valetk@bakermckenzie.com.*

Brian Hengesbaugh *is a partner and chair of Baker McKenzie's global privacy and security practice group based in Chicago. He focuses his practice on global data privacy and data security issues in business transformations, compliance activities and incident response/regulatory inquiries. He can be reached at brian.hengesbaugh@bakermckenzie.com.*

Baker McKenzie.