The Employment, Compliance & Privacy Report

Beckstead Terry PLLC

Getting Ready for the CCPA: Practical Action Items for Compliance

By Jana Terry, September 30, 2019

If your company is not ready for the California Consumer Privacy Act (the "CCPA"), you are in good company. According to one recent survey, 56% of companies polled will not be able to meet the California Consumer Protection Act's requirements when the law goes into effect January 1, 2020.[1]

But even if you can't be ready by January 1, there is no reason not to get going. As the Chinese proverb says, "The best time to plant a tree is twenty years ago. The second best time is now."

If you have determined that your business must comply with the CCPA, here is a list of action items that will help you get ready:

1. Understand the "big picture" of the CCPA.[2]

The main point of the law is to establish that California residents have

- the right to know what personal information is collected about them and to whom that information is sold/disclosed,
- the right to access their personal information and, sometimes, have it deleted,
- the right to opt out from sales of their personal information and
- the right not to be discriminated against for exercising their privacy rights.

[1] "PossibleNOW™ Survey: As California Consumer Privacy Act Enforcement Approaches, 56% of Businesses Report They Will Not Be Fully Prepared," August 30, 2019, https://www.prweb.com/releases/possiblenow_survey_as_california_consumer_privacy_act_enforcement_approaches_56_of_businesses_report_they_will_not_be_fully_prepared/prweb16512360.htm.

[2] This article summarizes and highlights CCPA obligations but is not a substitute for the CCPA itself, which is lengthy and complex. The CCPA is set forth in California Civil Code 1798.100-1798.199. It can be accessed online at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=

Although the title of the law makes it sound like it is aimed at the retail/"consumer" context, it is not that limited. **Under the CCPA, "consumer" means "a California resident."** Essentially, the CCPA is a comprehensive privacy regime—similar to the GDPR in Europe—that benefits the residents of California and makes covered businesses responsible for not only respecting the rights established but actually notifying California residents of their rights and helping them exercise their rights.

2. Assemble a team and take a data inventory.

If you have never gone through the process of mapping your company's data, this is the critical first step of any privacy compliance project. You need to be able to map the life cycle—from beginning to end—of the data at issue. For the immediate purpose of complying with the CCPA, you will want to identify the who, what, when, where, how, and why of data that relates to California residents:

- What kinds of personal data does the company have regarding California residents (data contained in email, employee/HR records, customer lists, etc.)?
- What are the points of collection? Where does the data come from? Emails? Online forms? Product orders? Phone calls? Lists from affiliates or third parties?
- What are the sources for the data?
- Can the California-related data be segregated from the other data?
- What systems/servers/platforms/devices hold the data?
- Who has access to those systems/servers/platforms/devices?
- How is the data secured?
- Why is the data collected? How is it used? For what purposes?
- Is the data disclosed, shared, sold or otherwise made available to any third party?
- Under what circumstances? To what third parties? For what purposes?
- Are the third parties under any contractual obligations with respect to how they handle the data?
- What privacy, information security and document retention policies are used by the company? When are they reviewed, monitored or tested?

3. Decide whether to take a California-specific approach.

Once you know how much personal information your company holds about California residents and how easy/difficult it will be to treat that data differently from other data, you will need to decide whether you want to take a California-specific approach or an across-the-board approach. Of course, the requirements of the CCPA only apply to the personal information of California residents. (Even if the business is located in California, the business need only comply with the CCPA for the personal information of California residents). In many cases, it will make sense to identify and segregate the California-specific personal information held by the company so that the new CCPA-compliant policies and procedures will apply only to that data. On the other hand, if a large part of your business is in California or if data segregation will be complicated, you may decide that it will be easier and cheaper in the long-run to apply the principles of the CCPA across-the board—regardless of consumer domicile.

4. Determine if your company "sells" California residents' personal information and if so, whether it really wants to continue.

For some businesses, selling data is an important part of the business model. The monetization of data is the lifeblood of companies like Facebook and Google. But for many businesses, selling data is just an additional revenue stream. If this is the case for your business, you probably want to consider whether that revenue stream is worth all the trouble presented by the CCPA. The most onerous and complex obligations of the CCPA apply to sellers of data. For example, "sellers" have to provide an opportunity for consumers to "opt out" of the sale of their data. The opt-out "button" (titled "Do Not Sell My Personal Information") has to be conspicuously displayed on the company's homepage. *Does your company want to put that button on its home page?* The personal information of children under age 16 is a different story. That data cannot be sold unless there has been prior *opt-in* consent.

For companies that want to sell personal information of California residents, the compliance requirements are going to be significant—and beyond the scope of this article. The easiest and cheapest way out of those obligations is to not sell data.

However, "sell" is broadly defined in the CCPA. It means "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating . . . a consumer's personal information . . . for monetary or other valuable consideration." In order to confirm that your company is not "selling," you need to make sure that the business is not receiving any "valuable consideration" in exchange for disclosure of personal information.

5. Determine what policies, processes, and tracking systems your company should implement in order to meet the CCPA's obligations.

In order to determine what policies, processes, and tracking systems you will need to put in place, you need to understand the range of compliance obligations established by the CCPA. The charts below identify (a) the CCPA's requirements for businesses and (b) suggested action items for meeting those obligations:

CCPA Requirement	❖ **Give Notice of Data Collection** Before collecting personal information from California residents, businesses must inform them of both • the categories of personal information that will be collected and • the purposes for which the personal information will be used. Businesses cannot collect additional categories of information (or use it for other purposes) without providing additional prior notice.
Compliance Action Items	➢ From the data inventory, **identify the categories** (from the statute) **and purposes** for collecting California residents' personal information. ➢ **Prepare a notice** containing this information. Confirm how the notice will be provided prior to collection of personal information pertaining to California residents. ➢ If you are implementing the CCPA only for California residents, you need to ensure that the company is able to **distinguish California residents** at the point of data collection. ➢ **Update the privacy policy** • to prohibit collecting or using personal information for purposes other than those disclosed in the notice and • to prohibit collecting additional categories of information without including those categories in the notice. ➢ **Implement procedures** that will help enforce the policy. For example, require review by privacy personnel any time there are website changes.

CCPA Requirement	❖ **Designate Methods for Consumers to Submit Requests.** Under the CCPA, consumers have the right to request information and to request that information be deleted. Businesses must provide at least two ways for consumers to exercise these rights. One of these methods must be a toll-free phone number. (However, if the recently-passed amendments are signed into law, businesses that operate exclusively online may designate an email address instead of a toll-free phone number). If the business maintains a website, a second method must be a website address. Consumers must be able to use the designated methods to exercise any and all of these rights: ➢ **The right to know** 1. the categories of personal information collected about the consumer (the "categories" are identified in the statute); 2. the categories of sources from which the personal information is collected; 3. the business/commercial purpose for collecting (and selling, if applicable) personal information; 4. categories of third parties with which the business shares personal information; and 5. specific pieces of personal information the business has collected. ➢ **The right to receive** 1. A list of the categories of personal information about the consumer that has been *sold* in the preceding 12 months and the categories of the third parties to whom the information was sold (or a statement that such information has not been sold) and 2. A "separate" list of the categories of personal information about the consumer that has been *disclosed* for a business purpose in the preceding 12 months and the categories of the third parties to whom the information was disclosed (or a statement that such information has not been disclosed for a business purpose). ➢ **The right to request deletion of personal information**
Compliance Action Items	o Establish a **toll-free phone number** to receive consumer requests. (If your business operates exclusively online, confirm whether the amendment that would permit you to designate an email address, instead of a toll-free phone number, is signed into law by October 1, 2019). o Decide what sort of **intake process** will be used and develop a form to be completed for each consumer request. o Work with website designers and IT to **create an online method** for making the requests and verifying the identity of the consumer. o Ensure that the personal information provided in the consumer request process is kept separate from other personal data (as it cannot be used for any other purpose).

CCPA Requirement	❖ **Be Able to Verify Consumer Requests** Businesses should only disclose personal information to consumers that make "*Verifiable* Consumer Requests." This means that the business must be able to verify that the consumer making the request is the same consumer about whom the business has collected personal information (or someone lawfully authorized to act on the consumer's behalf). The process and procedures involved in this verification process are critical because if personal information is disclosed to someone other than the correct consumer (or a properly authorized representative), the disclosure is a data breach.
Compliance Action Items	○ **Determine the process by which you will verify** that the person making the request is actually the consumer – particularly if the consumer does not have an account (and the business has no data against which to authenticate the information the consumer is providing). This is a very important step in the process. If done improperly, the requesting process becomes an avenue for data breach. *The business cannot provide personal information if the consumer request is not verifiable.* ○ **Create a written policy** reflecting the verification process. What information / combinations of information will be adequate for verification? If the verification cannot be immediately established, what process will be employed to request further information? At what point will it be determined that the consumer's request cannot be verified? ○ **Implement the verification policy through procedures**. For consistency, create a documentation process that will be completed for each request.

CCPA Requirement	❖ **Respond to Verifiable Consumer Requests in the Time and Manner Required:** ➢ Businesses are required to respond to verifiable consumer requests within 45 days (or within an additional 45 days (or even 90 days for particularly complex cases)) if notice is provided to the consumer along with reasons for the delay). ➢ If the business has statutory grounds to deny the request, the business must notify the consumer of the decision and rationale within the required time period. Note, for example, that the right of deletion is subject to a variety of listed exceptions. ➢ Additionally, businesses are not required to respond to a consumer more than twice in one 12-month period, and the personal information provided in response to the request need only cover the immediately preceding 12-month period. ➢ Where a consumer has made a request for disclosure, the manner in which the business responds depends upon whether the consumer has an account with the business. If the consumer has an account, the personal information should be delivered through that account. (However, note that the business cannot require a consumer to set up an account in order to submit their verifiable consumer request). If the consumer does not have an account, the information can be delivered by mail or electronically at the consumer's option. If the personal information is delivered electronically, it should be in a portable and readily usable format.
Compliance Action Items	○ Determine what personnel will be responsible for: • receiving the requests, • verifying the requests, • determining the business's response to the requests (including determining whether exceptions apply), • determining whether additional time will be needed, and • communicating with the consumer. ○ Implement a system for tracking consumer requests. Some sort of ticket should be created for each request and a system should be employed to move the ticket through the verification, decision-making, and communicating process. The system should be able to flag consumers that have already made 2 requests in the preceding 12 months. ○ Create a written policy for the business's response process. The policy should encompass how information is identified and gathered, how the business examines potential exceptions and grounds for denial of requests, how the business will communicate with the consumer, how each step will be documented and how/where the documentation will be retained so as to demonstrate compliance. Procedures should be implemented to ensure that the policy is followed.

CCPA Requirement	❖ **Update Privacy Policies to Include Required Information** Both the business's privacy policy and any California-specific description of consumers' privacy rights must include • designated methods for consumers to submit their CCPA-permitted requests, • a specific description of their CCPA rights of disclosure, non-discrimination, deletion, and opt-out, • a list of the categories of personal information collected about consumers in the preceding 12 months, and • two separate lists of categories of personal information the business has sold or disclosed for a business purpose within the preceding 12 months or, the fact that no personal information has been sold or disclosed, if that is the case. These policies have to be updated every 12 months.
Compliance Action Items	○ Carefully incorporate descriptions of the CCPA rights into your privacy policy. Stick to the language of the statute where possible. Look to any guidance provided by the Attorney General. ○ Generate the required lists. Ensure that the categories account for all data identified during your inventory. ○ Set up a process for monitoring compliance with your policy. Remember that, in addition to compliance with the CCPA, any representations made to consumers in your privacy policy can be enforced by the FTC. It is important that the representations made in the policy reflect what is actually happening.

CCPA Requirement	❖ **Do not discriminate against consumers who exercise their rights.** ➢ Under the CCPA, businesses cannot discriminate against consumers who exercise their rights. For example, the business cannot deny goods or services to consumers that opt out of the sale of their data. The business also cannot charge different prices (including offering discounts to those who do not opt out), vary the level or quality of goods or services, or suggest that the consumer will receive a different price, level or quality based on whether they provide personal information. ➢ However, the business *can* charge different prices or provide a different level or quality of goods or services if that difference is "reasonably" and "directly" related to the value provided to the business by the consumer's data. ➢ Further, a business *can* offer a financial incentive for the collection, sale or deletion of personal information so long as (i) the consumer has been notified of the material terms of the incentive, (ii) the consumer has provided prior "opt-in" consent, and (iii) the financial incentive practice is not unjust, unreasonable, coercive or usurious. Note that the statute provides that consumers can revoke their opt-in consent at any time and, in such case, they are not required to return the financial incentive received by the consumer. In other words, under the CCPA, it appears that consumers can opt-in for purposes of obtaining the financial incentive, then revoke the opt-in consent and retain the financial incentive.
Compliance Action Items	○ Determine whether the company offers discounts or other financial incentives in exchange for email addresses or other personal information. ○ Determine whether the company wants to continue these practices. Will it be possible for the company demonstrate that the value of the discount is "reasonably" and "directly" related to the value of the data provided? How? Will it be feasible for the company to meet the prior opt-in requirements for the financial incentive programs? ○ If the company wishes to continue offering discounts/financial incentives to people not residing in California, there needs to be a process in place that will distinguish California residents and prohibit their inclusion in the program.

CCPA Requirement	❖ **Train Personnel** The CCPA includes an independent requirement that companies provide training in specific areas to the employees who will handle consumer inquiries about privacy rights. Under the CCPA, companies are required to train employees regarding • how to instruct consumers to exercise their rights of disclosure and opt-out and • the general obligations of the CCPA as it pertains to non-discrimination, the business's disclosure obligations, and the business's duties regarding opt-out.
Compliance Action Items	○ All personnel that will handle consumer inquires regarding privacy and CCPA-permitted requests for disclosures or deletions need to be trained regarding the requirements of the CCPA. The "general obligations" of the CCPA are complex so the training needs to be fairly intensive. ○ Training should be mandatory for these employees and 100% compliance should be documented. ○ Personnel should be provided with all applicable policies and procedures and the training should include table-top exercises. ○ Additionally, companies need to make sure that its personnel understand the *company's* rights under the CCPA, which contains a number of exemptions and the sometimes-applicable "business purpose" exception. ○ Further, employees need to be mindful that the transparency goals of the CCPA will sometimes be in tension with other important values (such as the need to conduct investigations without the subject knowing the details of the investigation, the need to comply with subpoenas, and the importance of avoiding inadvertent data breach in the effort to comply with the disclosure obligations in the CCPA). Employees must be trained to recognize these potential issues/conflicts and know how and where to escalate these matters.

CCPA Requirement	❖ **Disclose Personal Information to Service Providers Only Pursuant to Written Contracts with Required Provisions** ➢ In the ordinary course of many businesses, personal information of consumers is shared with third party service providers (e.g., credit card processors, banks, shipping and fulfillment companies, companies that provide platforms for electronic transactions). ➢ Whenever personal data is shared with a service provider, it must be done **for a business purpose** and **pursuant to a written contract** that prohibits the service provider from retaining, using or disclosing the personal information for any purpose other than performing the specified service.
Compliance Action Items	o Using the data inventory, identify all service providers with whom personal information of California residents is shared and document the business purposes. o Determine whether, in the form by which the information is shared with the service provider, the personal information of California residents can be distinguished/segregated from other personal information? If not, consider across-the-board compliance with the obligations regarding disclosures to service providers. o Ensure that there is a written contract in place with each service provider that receives California residents' personal information. o Ensure that the written contract prohibits the service provider from retaining, using or disclosing the personal information of California residents for any purpose other than performing the specified service.

6. Take Advantage of "Safe Harbors"

There are several ways to avoid many of the onerous requirements of the CCPA. Consider these three:

a. **Don't retain data that you don't need**. The CCPA does not require businesses to collect personal information that it would not otherwise collect in the ordinary course of its business, retain personal information for longer than it would otherwise retain such information in the ordinary course of its business, or reidentify / link information that is not maintained in a manner that would be considered personal information. More particularly, the CCPA provides that, so long as a business is not selling or retaining the information, a business need not retain any personal information that is collected for a single, one-time transaction. Unless it is important to your business model to retain personal information (such as records of purchase histories concerning consumer accounts), one way to comply with the CCPA (or at least decrease the number of applicable obligations) is simply to ensure that the business is not selling or retaining any of the personal information that it collects in one-time transactions.

b. **Use only aggregated and de-identified data**. Under the CCPA, data is personal information only if it can be associated with a particular person. The CCPA makes clear (in an amendment likely to go into effect) that data that has been "aggregated" or "deidentified" is not personal information. Therefore, such data can be lawfully collected, used, retained, sold or disclosed without having to comply with the CCPA's requirements for personal information. If your company holds or sells aggregated or deidentified data, your compliance obligation with

respect to that data is simply to confirm that the data is aggregated or deidentified as defined by the statute.

c. **Encrypt and redact**. As mentioned above, the CCPA gives consumers the right to sue for data breaches, even if they cannot prove that they suffered actual damages. Consumers are required to give businesses notice and an opportunity to cure before filing suit, but in many cases it will not be possible to "cure" a data breach. As data breaches are more a question of *when* rather than *if,* and as the bell cannot generally be "un-rung," the potential exposure for companies is significant, particularly given California's propensity for class actions. However, it is important to note that the CCPA's data breach provisions (including the private right of action) kick in only if the compromised data is nonredacted and unencrypted. Investing in the latest encryption and redaction technology—*and training and monitoring employees to ensure that the technology is always used*—is an important risk mitigation strategy. Also remember to carefully secure the encryption keys.

7. Monitor Ongoing Developments.

On September 13, 2019, the California legislature passed several amendments to the CCPA. Assuming these amendments are signed into law by the Governor (which is expected), they will be effective when the law itself goes into effect on January 1, 2020. As some of the amendments will significantly impact the *degree* to which employers and business-to-business companies will have to comply (and the *ways* in which other businesses will be required to comply), it is important to confirm that the amendments are actually going to become law. Calendar October 13, 2019 as the date to check the status—that is the date by which the Governor must sign the amendments.

Additionally, the Attorney General has been tasked with promulgating regulations to further the purposes of the CCPA. The Attorney General's office has stated that it will release draft regulations in the "fall of 2019." If you go to https://oag.ca.gov/privacy/ccpa/subscribe, you can subscribe to an email list by which you will receive notifications of the Attorney General's rulemaking process. Although final regulations may not be published until July 2020, the draft regulations will provide helpful guidance concerning how to prioritize compliance efforts.