



CCPA Advent: Waiting on the World to Change

December 20th, 2019 | and [Webb McArthur](#)

January 1, 2020, opens both a new decade and a new landscape in privacy regulation in the United States. On that day, the California Consumer Privacy Act, or CCPA, is set to become effective. The law will be the first of its kind in the U.S., either at the federal or state level, in that it is set to regulate the collection and disclosure of an extraordinary range of personal information by any kind of for-profit business. The law will stand in contrast to other laws that regulate only limited types of personal information (for example, state data breach notification laws) or that only apply to certain business sectors. While many have compared the CCPA to the European Union's General Data Protection Regulation, it is a different beast entirely, and it stands as a warning – with other states likely to follow – that all businesses need to think seriously about data hygiene and privacy.

Businesses face challenges tackling the CCPA because the text of the law contains contradictions, ambiguities, and unique compliance challenges. Proposed regulations add some clarity but also raise new issues. The regulations will not be finalized until next year and could change. But with January 1, 2020 approaching, all businesses, including financial institutions, should take the law seriously.

Financial institutions should consider the following ten questions on assessing their CCPA readiness:

1. Are you a CCPA-regulated business?

The first question is whether or not you are regulated by the CCPA as a business. The CCPA applies broadly, but it applies only to for-profit businesses that do business in California and meet one of three size thresholds. (Make sure you check out Cal. Civ. Code § 1798.140(c).) If you are covered by the law, your parent company or your subsidiaries may also be wrapped into the scope of the law. If you don't meet one of the thresholds, you can breathe easily, but make sure you check back because these thresholds are likely to change in the future.

2. Do you act as a service provider?

Do you ever act as a service provider, such as providing support or analytic services to another financial institution? If so, there are two things to note. First, even if you don't meet one of the size thresholds discussed above, you may still be subject to the CCPA. Second, if you are subject to the law, you may only have limited obligations. You should discuss these situations with qualified counsel.

3. Have you completed your data inventory?

The most important step in complying with the CCPA is completing a data inventory exercise to capture all personal information regulated by the law. Remember that the law protects all California residents, whether they relate to you as your customer, your vendor, your employee, or any other role. The data inventory will allow you to know how to search across databases and systems to identify personal information for the purpose of fulfilling a consumer request under the law.

4. What personal information do you collect that is regulated by GLBA?

The biggest relief for financial institutions is that personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (“GLBA”) is exempt from the CCPA (with the exception of the private right of action for certain data breaches). You’ll want to make sure you know all your personal information that is regulated by GLBA, since it may be stored in different places and collected at different points. This also may be a good time to review your GLBA compliance procedures.

5. Do you have your Notice at Collection ready for employees?

If you have employees that are California residents, you’ll need to make sure that you provide them with the Notice at Collection discussed at Cal. Civ. Code § 1798.100(b) even though information about them may be exempt from other parts of the law. You will want to have this notice ready for any new data collection from employees.

6. Have you updated your online privacy policy?

Your online privacy policy reflects the work you have done to comply with the CCPA. Depending on the extent to which you are subject to the law, you may have to provide more or less information in your online privacy policy. But because your online privacy policy is public-facing, you should make sure you address these requirements with qualified counsel.

7. Have you reviewed your vendor agreements?

The advent of the CCPA will also be a good time to review your vendor agreements. For information regulated by the CCPA, you will want to make sure you have CCPA-compliant service provider agreements so that you can continue to provide your service providers with personal information after a consumer’s opt-out request. For information not regulated by the CCPA, it may be useful to formalize your understandings relating to CCPA compliance with your vendors.

8. Have you completed a status check on your data security procedures?

This is also a good time to do a data security check. Like we mentioned above, the CCPA provides for a private right of action to consumers injured by certain data breaches of unencrypted and unredacted data. The CCPA also expects you to properly secure personal information when verifying consumers for CCPA requests and in transmitting personal information. Talk with your IT and security teams about encryption and how else you can best protect the security of personal information in your control.

9. Have you reviewed your data retention practices?

The CCPA is meant to encourage, among other things, good data hygiene, so use this opportunity

to review your data retention practices and your old and offline personal information. The CCPA does not require you to keep any personal information you otherwise, in the ordinary course of business, would not keep, so it may be time to clean out a bit. Managing the entire life cycle of your data in an organized fashion will ease your compliance with the CCPA and lower your compliance risks generally.

10. Are you tracking the developments with the OAG?

The California Attorney General has a webpage dedicated to the CCPA. You will want to sign up for emails at <https://oag.ca.gov/privacy/ccpa> to get updates about finalized regulations and other CCPA matters. CCPA compliance will be a process you will have to revisit, so if you haven't begun, now is the time to start.