The Employment, Compliance & Privacy Report

Beckstead Terry PLLC

Texas Businesses Don't Need to Worry about the California Consumer Privacy Act , Right? *WRONG!* The Top 5 Misconceptions De-Bunked

By Jana Terry, September 16, 2019

California's legislature just finished its legislative session so the CCPA (the California Consumer Privacy Act) is back in the news. When the CCPA was (somewhat unexpectedly) enacted last year, many critics complained of the CCPA's various ambiguities and technical problems that would need to be corrected with amendments. Assuming that many changes would be made to the law before it went into effect, many businesses opted to put the CCPA on the back burner – at least until the law stabilized into a more final version. Other businesses assumed that they didn't need to worry about the CCPA because they thought it didn't apply to them.

If you were waiting for a "final-ish" version of the CCPA to emerge, your wait is over. The California Legislature just passed the only amendments that, if signed into law by Governor Newsom, will affect the CCPA when it goes into effect on January 1, 2020. If you haven't given the CCPA too much thought because you didn't think it would apply to businesses outside of California, think again.

These are the top 5 misconceptions about the reach and scope of the CCPA:

Misconception 1: Our business doesn't sell anything to individual California consumers, so we don't have any data that is governed by the law.

***Reality*:** Obviously the California *Consumer* Privacy Act is aimed at the personal data of "consumers." But it's not strictly a consumer protection law.

Consumer = California Resident

Under the CCPA, a "consumer" is any individual California "resident." (And a "resident" is anyone who is in California for other than a "temporary or transitory purpose" or who is domiciled in California but is outside the state for a temporary or transitory purpose). In other words, the law

applies in all kinds of contexts – not just the retail/consumer context. And when you think about it, all companies, even strictly business-to-business companies, hold data about people, whether those people are contact persons for business customers and service providers, job applicants, employees, contactors, tenants, family members, insureds, etc. The CCPA is a far-reaching law that applies to the personal information of all people who reside in California.

"Personal Information" defined:

Under the CCPA, personal information includes everything you can imagine The CCPA defines personal information as anything 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."

Examples of "Personal Information":

- real name or alias
- mailing address
- email address
- telephone number
- online identifier
- IP address
- social security number
- driver's license or state ID number
- account name
- signature
- insurance policy number
- credit card, debit card and bank account numbers
- physical characteristics or descriptions
- characteristics of protected classifications under California or federal law
- education information
- professional or employment-related information
- medical and health insurance information
- commercial information (records of personal property, products and services purchased or considered and other consuming histories or tendencies)
- biometric information
- internet or other electronic network activity (browsing history, search history, and interaction with a website, app or advertisement)
- geolocation data

The statute truly runs the gamut.

Finally, the information does not need to be accurate or true to count as personal information. If any personal information is used to draw inferences for the creation of consumer profiles, the inferences/profiles count as personal information—even if they are wrong.

Misconception No. 2: Our business has no locations in California, so the CCPA doesn't apply to us.

Reality: It is true that the CCPA does not apply if *every aspect* of the collection or sale of the California resident's personal information takes place "wholly outside of California" or if the company is not doing "business in the state of California." **But if companies have any nexus to California (and if they have California residents' personal information, they likely do) then they will probably fail the exemption tests.** For example, if a business collects any personal information from a California resident while they are in California or if any part of a sale of a California resident's personal information occurs in California, then the transaction is not "wholly" outside of California. As for the second test, under California law, an out-of-state business does business in California if it "actively engag[es] in any transaction for the purpose of financial or pecuniary gain or profit." This is interpreted very broadly. Any company that enters into contracts with companies or persons in California, or that employs persons in California, will be deemed to be doing business in California for purposes of the CCPA.

Misconception No. 3: We don't hold enough personal information of California residents to come within the scope of the CCPA.

Reality: **A business holding the personal information of even a single California resident may be subject to the CCPA**. In general, if your company is a for-profit business that receives (by any means) personal information pertaining to a California resident (or if some other company collects such information on your company's behalf), your business is the subject to the CCPA if *any* of the following criteria are met:

(1) The company receives, sells, or shares for commercial purposes, the personal information of at least 50,000 California residents, households or devices annually;
(2) The company derives 50% or more of its annual revenues from selling California residents' personal information; or
(3) The company has annual gross revenues in excess of $25 million.

Given the broad scope of the CCPA's definitions of "commercial purposes" and "selling," it will be easier for businesses to reach the thresholds identified in (1) and (2) than you might think. But the third criteria (annual gross revenues in excess of $25 million) is the one that will capture the most businesses. Although the CCPA does not make explicit that "annual gross revenues" means total world-wide revenues, it also does not limit the revenues to those generated in California (which is in contrast to criteria (1) and (2)). And unlike the California Revenue and Tax Code, which applies only to income "derived from or attributable to" California, there is wide agreement that, for purposes of criteria (3), the revenues need not be generated in California. **In short, if your business generates, wholly outside of California, $25 million in annual gross revenues and holds the personal information of even one California resident, your business will be required to comply with the CCPA with respect to that data, unless some exemption applies**.

Misconception No. 4: We only have employee data and the CCPA is being amended to exempt that data from the law.

Reality: **It is true that on September 13, 2019, the legislature passed an amendment that will, if signed by Governor Newsom, *temporarily* exempt employers from having to comply with *most* provisions of the CCPA with respect to job applicant and employment-related personal information**. However, the exemption is only for one year and it does not give employers an across-the-board exemption. In particular, even if the employer exemption amendment is signed into law, employers will still be required to comply with the notice requirement and the data breach portion of the CCPA (which includes a private right of action).

It is also important to note that this exemption is for employers; it does not apply to the entire employment context. Specifically, the amendment excludes from most CCPA requirements personal information that is retained by a business for the purpose of administering benefits for ***its own*** employees or contractors, to the extent that the information is collected and used solely within the benefits administration context. Further, the amendment also applies to personal information (including emergency contact information for other persons) that is collected from job applicants, employees, owners, directors, officers, medical staff members or contractors, but only to the extent that the personal information is collected and used solely within the context of having emergency contact information on file or solely within the context of their roles or former roles as job applicants to, employees of, owners of, directors of, officers of, medical staff members of, or contractors of ***that business***. As drafted, this amendment does not seem calculated to benefit any of the other non-employer entities that collect personal information from job applicants and employees. For example, recruiters collect personal information from job applicants, but unless the job applicant becomes an employee or contractor *of the recruiting firm*, the recruiting firm will not benefit from this amendment. Similarly, benefits providers will not be covered by the amendment, except with respect to its own job applicants, employees, etc.

It is expected that Governor Newsom will sign the employer exemption amendment into law by the October 13, 2019 deadline. However, if for some reason that does not happen (or if the amendment passes but no further employer-exempting legislation passes prior to the amendment's sunset date of January 1, 2021), then the CCPA will dramatically increase California employees' rights. For example, while the California Labor Code currently gives employees the right to access their personnel files and records relating to their performance or grievances concerning them, such right of access is limited because it does not apply to letters of reference, records relating to an investigation of a possible criminal offense, or reports/ratings obtained prior to employment, prepared by examination committee members or obtained in connection with a promotional exam. By contrast, the CCPA does not specifically exempt such records from the definition of "personal information." Additionally, the right under the CCPA to request deletion of records will prove problematic when applied in the employment context. Finally, if the CCPA applies across the board in the employment context, employers will have to perform other independent obligations (such as training, ensuring that vendor contracts contain certain provisions, and creating methods for consumers/employees to assert their rights).

Exercise caution, however, before you conclude that the only personal information your B2B company holds regarding California residents is employee data. Personal information collected from business contacts is covered by the CCPA. The legislature passed an amendment to exempt that sort of information *for one year only* but, like the employer exemption, the one-year B2B exemption does not apply across the board. Companies that collect personal information from persons who are acting solely on behalf of a business still have to comply with the provisions concerning opt-out rights, non-discrimination, and the rights of consumers in the event of data breach.

Misconception No. 5: We already prepared for GDPR so we don't need to do any further work to comply with the CCPA.

Reality: If you are in compliance with GDPR, and you are applying GDPR across-the-board (not just to Europeans), you are definitely well-positioned. All of your prior efforts can be leveraged to achieve compliance with CCPA. However, there are some tweaks you may need to make.

Examples of CCPA consumer rights and business obligations that differ from the GDPR and may require attention:

(1) The Opt-Out Right: Under the CCPA, consumers have a right to "opt out" from the sale of their data. GDPR has similar rights (erasure and objection) but they are more limited. *If your company "sells" (as very broadly defined by the CCPA) personal information, have you put in place the specific notice and opt-out mechanisms required by the CCPA? (For example, do you have a link on the webpage titled "Do Not Sell My Personal Information"? Do you have a system in place to respect the opt-out decision for at least 12 months? Have you ensured that the data collected for opt-out purposes is not used for other purposes?)*

(2) The Non-Discrimination Obligation: The CCPA more explicitly prohibits discrimination against consumers that exercise their opt-out and other CCPA rights. *If you offer financial incentives (e.g., discounts, promotional items) to consumers who provide personal data, have you considered whether the practice is "discrimination" under the CCPA? In order to comply, you may need to provide additional notices and document the "direct" relationship between the value of the data collected and the value of the benefit given to the consumer.*

(3) Training Requirements: The training obligation is more specifically defined in the CCPA than in the GDPR. The CCPA requires training in specified areas (such as consumer rights to request information, consumer rights regarding the sale of data, the business's obligation to verify consumer requests before providing requested information, and the non-discrimination rules). *Does your training cover the areas required by the CCPA?*

(4) Obligation to Designate Methods to Exercise Rights: The CCPA requires businesses to designate methods by which consumers can exercise their rights. A toll-free number is required (although one amendment, if signed into law, will substitute an email address for a toll-free number in the case of businesses that operate exclusively online). Additionally, if the company maintains a website, the company must also enable exercise of rights through the website. *Do you have a toll-*

free number set up for use by California residents? If your company has a website, does it have an access point for the exercise of data rights?

Sources: California Consumer Privacy Act, Civil Code §§ 1798.100 – 1798.199; *CCPA Amendment Tracker*, International Association of Privacy Professionals, https://iapp.org/resources/article/ccpa-amendment-tracker/; California Legislative Information website providing full text of all amendments that passed (AB-25, AB-874, AB-1146, AB-1355, & AB-1564), https://leginfo.legislature.ca.gov; California Revenue and Taxation Code, § 23101.