We're Not Californians! Why Should We Care About the California Consumer Protection Act?

Mellisa D. Maxwell
Claire C. Rosston

If your business clients haven't already asked you about the California Consumer Protection Act (CCPA),[1] expect that they will soon. The CCPA is the first data privacy and security act in the United States with expansive protections for data that can identify or is directly or indirectly linked to particular individuals. Even though the CCPA applies to the personal information of California residents only, its reach will extend well beyond the borders of California.

Idaho businesses that collect or have access to personal information of California residents will fall within the CCPA's purview. The CCPA also imposes stiff penalties of up to $2,500 for each violation, which increases to $7,500 if the violation is intentional. Moreover, it gives California residents a civil right of action for injunctive or declaratory relief as well as monetary damages against businesses that fail to implement reasonable security measures to protect their personal information.

Given the liability for noncompliance and the likelihood that the CCPA will become the standard for best practices in privacy and data protection unless preempted by federal law or another state adopts more rigorous requirements, Idaho business lawyers need to understand the basic components of the CCPA to serve their clients well. This article outlines the components of the CCPA that every business lawyer should know, with the caveats that some interpretation challenges still exist and that additional amendments and regulatory guidance may be issued prior to the January 1, 2020 effective date.

Idaho businesses that collect or have access to personal information of California residents will fall within the CCPA's purview. The CCPA also imposes stiff penalties of up to $2,500 for each violation, which increases to $7,500 if the violation is intentional.

Broad application of the CCPA

In order to understand how the CCPA could apply to Idaho clients, it is important to recognize the broad group of entities that are within its scope. First and foremost, the CCPA applies to any for-profit business (regardless of where it is located) that controls personal information of California residents and satisfies at least one of the following criteria: (i) generates gross revenues above $25 million; (ii) annually receives or shares for commercial purposes or buys or sells personal information of at least 50,000 California residents, households, or internet-connected devices; or (iii) derives at least 50% of its annual revenue from selling California residents' personal information.

A business controls California residents' personal information if it determines the purposes and means of processing the personal information that is collected by it or on its behalf. As a result, a business can be covered by the CCPA even if it does not itself collect and store California residents' personal information. For example, your client hires a consulting firm to survey its California employees about their job satisfaction, and in doing so, instructs the consulting firm which questions to ask and how it wants the results communicated in charts and summaries that de-identify the data. Despite not directly collecting, processing, or storing the personal data, your client is the controller of the data.

In addition, the CCPA covers more than just businesses that control personal information. All businesses that are controlled by or share common branding with a business covered by the CCPA must comply with the CCPA, regardless of whether such businesses independently satisfy the criteria for covered businesses.

Finally, the CCPA also applies to any service providers or other individuals and entities (regardless of location) who purchase or receive personal information of California residents for a business purpose. Therefore, while your clients may not be businesses as described above, the CCPA may affect them based on what the regulation identifies as a "service provider" or a "third party."

A service provider is a for-profit entity that processes information on behalf of a CCPA-covered business. If your client operates under a business-to-business model, requirements may be pushed down to your

client pursuant to a written contract. On the flip side, if your client is a covered business, it will want its vendor contracts to contain certain restrictions and obligations because the regulation may offer some protections to the business if its contracts contain the required terms.

Unlike a business or a service provider, the regulation defines a "third party" in the negative. Because of some subtle nuances, this results in a number of interpretive challenges. In short, however, a third party is any person or entity that is not a business or service provider. However, a situation could arise when a client is a service provider (*i.e.*, a vendor to a business) but is not a "service provider" as defined under the CCPA.

It is crucial to understand the relationships within the organizational ecosystem, the data involved, and the contractual terms in place among entities because the obligations and requirements under the regulation will vary. Falling into one category over another could impact your clients' ability to conduct business or add administrative burdens they may or may not be able to carry out.

Key definitions

The broad scope of the CCPA is largely derived from the key definitions of "personal information," "processing," and "selling." When it comes to consumers as individuals, they may have different ideas on what is considered private or personal. Simply asking clients or business owners if they are receiving, collecting, or storing personal information is problematic because each individual you are asking will likely attribute his or her own understanding as opposed to how the term is defined under the regulation.

Under the CCPA, personal information is any 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. Section 1798.140(o) of the CCPA provides an illustrative, but not exclusive, list of the categories of information within the definition of personal information. The categories include the expected identifiers, such as name, address, or SSN. However, identifiers also include IP address, email address, account names, and other similar identifiers.

Other categories that may not intuitively seem like personal information include commercial information; internet/electronic network activity information; audio, electronic, visual, thermal, olfactory, or similar information; professional or employment-related information; or inferences from any information that could create a profile about a consumer.

The broad scope of the CCPA is largely derived from the key definitions of "personal information," "processing," and "selling."

Fortunately, a few exceptions have been carved out from this very broad definition. One exception is "publicly available" information as defined under the regulation. There are also exceptions for information that is de-identified or aggregated in accordance with the regulation. Medical information is also excluded to the extent it is protected under the California Confidentiality of Medical Information Act. Similarly, protected health information (PHI) as defined and governed under the Health Insurance Portability and Accountability Act (HIPAA) is also excluded. While these carve-outs are helpful in theory, in practice it could be a large technical feat for clients to segregate data that is subject to HIPAA as PHI from information that is personal information under the CCPA.

The CCPA also uses the expansive terms "processing" and "selling." Even if your client is not directly covered by the CCPA because it does not control how personal data is collected and used, it may still be a service provider by virtue of processing personal data for another business. Service providers are required to comply with certain requirements of the CCPA that controllers of personal data contractually obligate them to do. The CCPA defines "processing" to mean any operation performed on personal data, regardless of whether it is by automated means. Something as simple as linking one piece of personal data with a customer identifier is sufficient to process the data.

The CCPA contains many restrictions related to the selling of personal information, including giving California residents the right to opt out of the sale of their personal information. Under the CCPA, the word "sell" and its variations are defined broadly to mean any disclosure, transfer, or making available personal information of California residents for monetary or other valuable consideration. Consequently, two business with a data sharing agreement are selling personal data to each other under the regulation by virtue of the exchange of the data, which has value, for other data.

Inventorying data

Inventorying data collected and stored by a business is the foundation of its compliance with CCPA. It is not possible for your clients to comply with the CCPA without knowing what personal data they collect, how the various pieces of personal data are linked to one another, and the purpose for collecting and storing the data. For this reason, the first step towards CCPA compliance is for your clients to inventory their data.

It is most likely that all employees of a business collect personal data in some form or another, even if this is done merely by storing contact information and signature cards in an employee's email account. Your clients should identify all data collection points and detailed information about the data collected. This can be done by asking each employee to answer a questionnaire about the data the employee collects and stores. This questionnaire should also ask specific information about the data in order to accurately categorize the data and how it is used.

Through this exercise, your clients should be able to answer the following questions about each type of data they collect:

1. Is the data personal information?
2. Within which category (*e.g.*, biometric or financial) does the data fit?
3. Is the data encrypted?
4. What is the source of the data?
5. How is the data used?
6. How is the data linked/tracked/connected with other data?
7. Is the data sold? If yes, to whom?
8. Is the data disclosed? If yes, to whom and for what purpose?
9. How long is the data retained?
10. Is the data discarded by destruction or de-identification?

With this information, a business can then prepare an easy-to-use reference illustrating the life cycle of all of the personal data it collects and stores and to which other data the personal data is linked. This reference can then be used for your client to consider whether it can change any of its personal data collection practices in order to lessen its CCPA compliance burden. It costs money to collect and store data. If your client doesn't need particular types of personal data, it can improve its bottom line and minimize its CCPA compliance burden by reducing what data it collects and how long the data is kept.

In order to demonstrate compliance with the CCPA, organizations must develop, implement, and maintain appropriate policies and procedures and other measures necessary to comply with the requirements of the law.

Updating policies and procedures

In order to demonstrate compliance with the CCPA, organizations must develop, implement, and maintain appropriate policies and procedures and other measures necessary to comply with the requirements of the law. Consumers must be offered at least two methods to submit requests and procedures must be implemented to process all requests in the manner and time frame prescribed. Some of these processes and procedures may be easy to implement; however, others may require significant changes depending on your client's business and past efforts to comply with data privacy and security laws.

The mechanisms employed and evidence used to demonstrate compliance with the following consumer rights may vary depending on the nature and size of your client. One of the largest compliance burdens is for businesses to be ready to respond to the consumer rights granted by the CCPA. The basic consumer rights covered under the regulation are: (1) the right of access; (2) the right to erasure; (3) the right to not be subject to discrimination; (4) the right to data portability; (5) the right to object; and (6) the right to be informed.

The less technical implementations include providing consumers with full visibility of the data the organization has about them. This means each consumer has the right to obtain details, and even copies, of such data. A process must be in place to handle all requests in the manner and time frame prescribed.

In addition, consumers have a right to request deletion of their personal information free of charge (although there are times when a fee may be requested). Also, if incentives are offered for the collection, sale, or deletion of information, then policies and procedures must be in place to provide consumers with notice of the financial incentives, and consumers must expressly opt in to any such incentive programs. This ties into the requirement that consumers may not be discriminated against for opting out of the sale of their personal information.

When it comes to the data portability requirement, consumers have a right to obtain access to their data in a format that allows the transmission of the data to someone of their choice without hindrance or cost. Your clients must have mechanisms in place to validate the identity of individuals requesting this information. More technical compliance requirements include a "Do Not Sell My Personal Information" link and extensive employee training.

Lastly, certain information must be provided to individuals, informing them of their rights under the CCPA. One way to inform consumers is through the privacy notice and published privacy policy, which means businesses will need to update their privacy policies to comply with the CCPA's considerable notice requirements.

Updating privacy policies

Under the CCPA, your clients must disclose practices related to the collection and use of California residents' personal information. In particular, a business' privacy policy must include the categories of personal information that the business has collected and the personal information that the business has sold or disclosed for a business purpose in the preceding 12 months.

Additionally, the CCPA requires notice of the rights the CCPA gives California residents with respect to their personal information and how they may exercise these rights by making requests to a business about their personal information. Your clients also need to make sure that their websites contain multiple ways for the individuals to exercise their rights, including, at a minimum, a toll-free telephone number and a website address.

Takeaway

At the end of the day, even though the CCPA applies only to businesses with customers or employees who are California residents, businesses will likely find it cumbersome to maintain separate processes for California residents. Given the shift on the national stage regarding privacy, all of your clients should consider implementing these requirements as best practices sooner rather than later, recognizing that the CCPA will likely become the standard for U.S. residents everywhere.

Given the shift on the national stage regarding privacy, all of your clients should consider implementing these requirements as best practices sooner rather than later, recognizing that the CCPA will likely become the standard for U.S. residents everywhere.

Endnotes

1. Stats. 2018, c. 55 (A.B.375), § 3, eff. Jan. 1, 2019, operative Jan. 1, 2020, as amended by Stats. 2018, c. 735 (S.B.1121). The CCPA, as amended, has not been codified. The CCPA is expected to be codified as Sections 1798.100 to 1798.199 of the California Civil Code. The CCPA's definitions are set forth in what is expected to be codified as Section 1798.140. The consumer rights granted by the CCPA are set forth in what is expected to be codified as Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, and 1798.125.

Mellisa D. Maxwell *is the Associate General Counsel and Privacy Officer at Healthwise, Incorporated and an Adjunct Professor at Concordia University School of Law. She currently serves as the Executive Director to Initium Law, Inc. where she also volunteers her time to provide legal services to small businesses, startups, and nonprofits. When not being a lawyer she is roaming around the wilderness with her adventure dog, a Staffy rescue.*

Claire C. Rosston *is a business attorney at Holland & Hart LLP who counsels clients in data privacy and security and commercial transactions, including business acquisitions and secured financings.*