

TYPES NOT MAPPED YET December 10, 2019 | TTR not mapped yet | Jennifer A. Post, Luke Sosnicki

CCPA: The next horizon for M&A deals in California and beyond

The California Consumer Privacy Act (CCPA) takes effect on January 1, 2020. Private litigants may begin to bring lawsuits under the CCPA for data breaches the same day. California's Attorney General will begin enforcing the CCPA in its entirety six months later on July 1, 2020.

Recent polls suggest that many companies covered by the CCPA are not yet compliant. Some report that they have just now begun to consider how the statute will affect them. This creates some interesting issues and pitfalls for M&A deals beginning in 2020, as the CCPA has important implications not just for covered businesses, but likewise for businesses acquiring or merging with those covered businesses.

CCPA overview

In general terms, the CCPA grants California consumers certain rights with respect to the personal information that covered businesses collect about them. Starting on January 1, 2020, California consumers will be able to ask covered businesses what personal consumer information the businesses collect and hold, what they do with it, and specifically whether they sell it. Consumers will further have the right to opt-out of the sale of their personal information, and may also request that businesses delete it (subject to a long list of exceptions as to the types of information that businesses may refuse to delete).

To comply with the CCPA, covered businesses must create internal processes and procedures to properly inform consumers of their rights, collect consumer requests and properly document them and then to honor consumer requests within the timeframes imposed by the statute. Perhaps most importantly, starting on January 1, 2020, California consumers will be informed of their right to demand that covered businesses stop selling their personal information. Many consumers will likely exercise that right.

Non-compliance with the CCPA is enforceable by California's Attorney General, punishable by fines of \$2,500 to \$7,500 per violation. The statute also provides a private right of action for data breaches, with statutory penalties of \$100 to \$750 per consumer per violation, or actual damages, whichever is more. These statutory liabilities will be quite significant if brought in the context of class-action or other large scale litigation.

What is a "covered business" under the CCPA?

The CCPA is not limited to California businesses. The CCPA applies to any for-profit entity that does business in California that: (i) generates more than \$25 million in annual revenue; (ii) collects information from 50,000 or more California consumers, households, or devices annually; or (iii) derives over half of its revenue from selling consumer information.

The CCPA also imposes obligations on service providers of covered businesses. The term "service provider" is a defined term that includes any for-profit entity (including various types of vendors) that receives consumer information from a covered business pursuant to a written contract stating what the service provider is to do with that information. While a service provider may not need to comply with all of the CCPA's provisions, service providers will need to implement opt-out and deletion requests. The draft implementing regulations also impose on covered businesses an obligation to ensure that any consumer data they are selling is collected from consumers who were properly notified of their rights.

How will the CCPA affect M&A transactions?

If your company is preparing for a sale, or is contemplating acquiring a covered business or service provider, at a minimum, you should be asking yourself the following:

Is the transaction itself a “sale” of consumer information under the CCPA?

The CCPA very broadly defines the term “sale” as it applies to consumers’ right to opt out. A “sale” is defined as “selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.”

The definition contains a carve-out for the transfer of information as an asset “that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business....” While this exception is likely to apply to most M&A transactions, the transaction documents should specifically reference the information transferred under this provision to minimize the risk that consumers’ opt-out rights will apply.

How does the subject company track the consumer information that it collects?

One of the first steps of CCPA compliance is data mapping. In order to comply with the CCPA’s notice and other provisions, a covered business must first understand: (1) what consumer information it collects, (2) how it collects the information, (3) how the information moves inside and outside of the business, and (4) whether or not the data is sold.

A covered business that collects, but does not adequately track consumer information simply cannot comply with the CCPA. In the context of M&A transactions, an acquiring company should carefully review the data-mapping practices of the target to ensure that all consumer data is accounted for, and carefully mapped, both within the company and at any point where it flows out.

What written contracts does the subject company have that “implicate obligations” under the CCPA?

Any covered business that sells or transfers consumer information to a buyer or third-party service provider must have written agreements that impose obligations under the CCPA.

For example, a covered entity that receives an opt-out request from a consumer must notify all parties to whom such information was sold within the prior 90 days. If a covered entity receives a deletion request, it must also convey that request to its agents and service providers. The buyers and service providers must then also comply with these requests—if they do not, the covered business may well be faulted for failing to ensure compliance.

An acquiring company should carefully review the target company’s agreements with its services providers and data buyers to determine if the target company has adequate rights to ensure that the target’s data buyers and service providers properly secure consumer information and themselves comply with the CCPA.

What is the value to the business of consumer information that it collects and/or sells and how can that affect the valuation of transactions?

Covered businesses involved in M&A deals will need to consider the value and monetization of the consumer information they collect, for at least two reasons.

First, the CCPA mandates that businesses selling consumer information provide clear notice to consumers of their right to opt out of such sales. Given the publicity that recent large data breaches have garnered, and growing concerns about privacy, generally, it is reasonable to assume that a good number of consumers will exercise that right. Businesses that derive material revenue from selling consumer information must be prepared to account for large-scale opt-out requests—and value it accordingly.

Second, the CCPA prohibits businesses from charging different fees or rates based on whether a consumer has exercised her or his opt-out (or other) rights unless those fees are directly related to the value of the consumer’s data. If a business intends to charge different rates based on the value of the data to its business, it must also explain to the consumer how that value is derived. The flipside is that if a business is charging consumers different rates that it cannot explain, that revenue stream may need to be revised.

Both of the above have implications for M&A valuations, where financial projections involve or center around material revenue from consumer data on the revenue side and the costs of CCPA compliance or compliance failure on the expense side. In addition, there may also be a significant cost to bringing a covered business into compliance. If the acquiring company has not built these costs and potential variations into its models, the cost of an integrating or realizing the benefits of an acquisition may well exceed projections.

How does the target company approach data security?

The CCPA’s private right of action for data breaches poses a risk of significant liability. With statutory penalties of \$100 to \$750 per consumer, per incident, a single large data breach followed by class-action litigation could be incredibly costly—and even smaller breaches could have a material effect.

In order to recover damages, a private plaintiff suing under the CCPA must show the breach resulted from the defendant’s failure to use “reasonable security procedures and practices.” While this standard will not be defined until cases start to wind their way through the courts, a baseline for showing “reasonable security” starts with a comprehensive data-security policy and well-defined procedures.

Because proving “reasonable security” may ultimately require convincing a trier of fact, the acquiring company should review not just how the target company protects its consumer data, but how clearly those procedures are documented as well.

Does the subject company currently comply with the CCPA?

The CCPA imposes numerous obligations on covered entities relating to the collection and sale of consumer information. Due diligence in M&A transactions involving covered companies now must include assessment of the following:

- **Privacy notices, including online privacy policy:** The CCPA requires covered businesses to provide the following notices to consumers (which may be combined): a notice of collection, a notice of the right to opt-out, a notice describing any financial incentives offered to consumers who permit their information to be used, and an online privacy notice. The draft implementing regulations contain detailed provisions as to when and how these notices must be provided, and what information they must contain.
- **Processes to collect and implement consumer requests:** Covered businesses must design and implement processes to receive, and comply with, consumer requests. These include right-to-know, opt-out, and deletion requests. Notably, different types of requests have different time-frames for compliance.
- **Recordkeeping and consumer complaints:** The CCPA requires covered businesses to keep records of consumer requests and responses for two years. It also requires larger businesses to include compliance metrics in their online privacy policies. As part of the due diligence process, a target companies’ metrics relating to CCPA compliance, as well as records relating to consumer complaints, must be carefully reviewed in order to assess the potential regulatory and private-litigation risks associated with the target’s business.
- **Training programs:** The CCPA requires covered businesses to train employees whose responsibilities include the business’ compliance with the CCPA. It also requires large entities to draft a written CCPA training policy. The due diligence process should include review and assessment of the training materials that target companies maintain.
- **What applicable cyber insurance does the subject company maintain?** While not a specific obligation under the CCPA, cyber insurance is an important aspect of preparing for the CCPA. As is the case generally for companies that own or use any confidential information belonging to third parties, review of the target company’s cyber insurance policies will be critical to assessing the value of any cyber risks.

Key implications for M&A transactions

While each transaction (including the sale of your own company) will require tailored due diligence and transaction valuation negotiations, in light of the CCPA, the following will certainly be important guideposts for transaction parties and their advisors in valuing transactions, designing targeted due diligence exercises and preparing documentation:

- Determining with certainty whether the seller or buyer (or any of its subsidiaries) is a “covered business” including entities headquartered outside of California
- Exploring structures that may cause the transaction to be exempt from the definition of data “sale” under the CCPA
- Evaluating the current compliance status of the subject company and therefore evaluating: costs to correct or maintain compliance, litigation risks, anticipated deviations from current revenue models and determination of whether applicable insurance could mitigate noncompliance risks
- Careful review of service-provider agreements to determine rights of enforcement as to CCPA requirements and related evaluation of service provider compliance
- Negotiating indemnification categories and creating holdbacks or protective escrows and determining the length of such obligations given ongoing statutory requirements
- Negotiating exclusions and coverages with respect to representation and warranty insurance, assuming such insurance is available for CCPA-related representations



- Educating equity investors and credit providers as to the risks and costs of CCPA compliance with respect to the subject company

For more information about the California Consumer Privacy Act and its implications for your business activities, please contact Luke Sosnicki and Jennifer Post.

authorsTest

jennifer

Jennifer A. Post

luke

Luke Sosnicki