Impact of the California Consumer Privacy Act on M&A

June 10, 2019

Introduction

Similar to the European Union's General Data Protection Regulation, the passage of the California Consumer Privacy Act ("**CCPA**") is ushering in a new era of data privacy and data security considerations in the United States as companies are preparing for its effectiveness, the possibility for follow-ons in other states and the potential for preemptive federal legislation. Since the CCPA's passage in 2018, the CCPA's requirements have been a focus for companies based not only in California, but throughout the United States and abroad due to its extraterritorial scope. While the CCPA does not become effective until January 2020, companies would be well served to evaluate now how the law's requirements may apply to them and impact their day-to-day operations, and, in particular, their M&A transactions.

We discuss below the transactional considerations for investors, purchasers and sellers of companies that collect or process personal data of California residents arising from the CCPA.

Executive Summary

- The broad scope of the CCPA will create compliance obligations for companies, regardless of domicile, that collect or process any of a wide range of types of personal information from California residents.
- The risk of costly and highly visible private actions will increase the importance of conducting thorough due diligence on a target's personal data practices, data security systems and compliance with the CCPA. Please see Annex A for sample due diligence questions to ask targets.
- Transaction structuring and risk allocation mechanisms should expressly contemplate data security and data management to ensure compliance, and allocate the risk of non-compliance, with the CCPA.
- Companies should monitor proposed amendments, forthcoming guidance from the California Attorney General, enforcement actions and court rulings to establish best practices.

Diligence Considerations: CCPA Scope, Compliance and Penalties

CCPA Scope

Purchasers and investors should first consider the extent to which a target is subject to the CCPA in order to determine whether the law's obligations apply to the target's collection, maintenance, sale or other transfer of personal information. The CCPA applies to certain businesses that collect personal information from California residents, who are defined as "consumers" under the CCPA.[1] For purposes of the CCPA, a "business" is any for-profit legal entity that (i) does business in California, (ii) collects, or directs others to collect, consumers' personal information and determines the purposes and means of processing of

[1] *See, e.g.*, Cal. Civ. Code tit. 1.81.5, § 1798.140(c) (2018).

consumers' personal information and (iii) (1) has annual gross revenues in excess of $25 million, (2) annually buys, sells or otherwise commercially processes the personal information of at least 50,000 consumers, households or devices or (3) derives 50% or more of its annual revenues from selling consumers' personal information.[2] An entity's obligation to comply with the CCPA flows to majority-owned subsidiaries or parent companies with common branding, even if those entities do not independently meet the qualifications of a "business" under the CCPA. As a result, evaluating whether a particular target is subject to the CCPA may require consideration of the activities of its subsidiaries or parent companies.[3] A business and a consumer do not need to engage in a commercial transaction for the business's collection of that consumer's data to come within the purview of the CCPA, so data intermediaries, partners and service providers may also be subject to the CCPA.[4]

"Personal information" is defined very broadly for purposes of the CCPA and encompasses nearly any information that could be linked, directly or indirectly, with a particular California resident or "household."[5] Personal information does not include information that is publicly available from government records, or de-identified or aggregated consumer information.[6] Additionally, with limitations, the CCPA does not apply to certain medical and clinical trial information, health care providers and other entities governed by the Health Insurance Portability and Accountability Act of 1996 breach notification rules, or personal information processed under certain privacy, security and other U.S. legal frameworks, such as the federal Fair Credit Reporting Act and Gramm-Leach-Bliley Act.[7]

CCPA Compliance

One key compliance consideration is whether the target "sells" personal information for purposes of the CCPA. If a business "sells" personal information, the business must affirmatively disclose to consumers that their personal information may be sold and that consumers have the "right to opt-out" of such sale and the business must respond to certain consumer requests.[8] A business "sells" personal information when the business transfers or otherwise communicates a consumer's personal information to another business or a third party for money or other valuable consideration.[9] However, the CCPA provides for certain exemptions to the scope of a covered sale.[10] For example, a business does not sell personal information when a consumer (i) directs a business to intentionally disclose the personal information or (ii) uses a business to intentionally engage with and provide personal information to a third party.[11] Moreover, a business does not sell personal information when (i) (a) it shares the information with a service provider pursuant to a written contract that prohibits the service provider from retaining, using or disclosing the personal information for any purpose other than the specific purpose of performing the services specified in the contract for the business[12] and (b) the service provider does not collect, sell or

---

[2] *Id.* § 1798.140(g).

[3] *Id.* § 1798.140(c)(2).

[4] *Id.* § 1798.140(o)(1).

[5] *Id.* § 1798.140(o).

[6] *Id.* § 1798.140(o)(2).

[7] *Id.* § 1798.145(c)-(f).

[8] *E.g.*, *id.* §§ 1798.20(b) and 1798.135(a).

[9] *Id.* § 1798.140(t)(1).

[10] *Id.* § 1798.140(t).

[11] *Id.* § 1798.140(t)(2)(A).

[12] *Id.* § 1798.140(v).

use the personal information beyond the scope of the services provided or (ii) that information is transferred as an asset as part of a merger, acquisition or other change in control of a business; however, if a purchaser materially changes how it uses consumer personal information as a result of a merger or acquisition, the purchaser must provide new notice of the changed practice to consumers.[13]

- Practice Tip: Review a target's agreements with its service providers to ensure that they contain contractual provisions that restrict use of the processed personal information to use in connection with performing the services specified in the contract and not for any other use. The exemption for service providers from the scope of a covered sale described above will be an important exception to keep in mind for ancillary agreements that may involve the transfer of personal information.
- Practice Tip: Look beyond the target's customer-facing business to consider possible obligations under the CCPA. As currently drafted, the law may apply to data collected by a company about its employees, contractors or even job candidates, if these individuals are California residents. Therefore, even a target that does not commercialize consumer data may still be subject to the CCPA if it collects routine human resources data about Californian employees, contractors or candidates. As a result, similar notice and consumer rights obligations may apply with respect to a target's employees.
- Practice Tip: For sellers, anticipate purchaser and investor CCPA diligence questions and consider practicing responses with outside counsel to describe what the seller has done regarding CCPA compliance. Given the current uncertainties regarding interpretation and enforcement, purchasers and investors will expect sellers to take a thoughtful and measured approach and be able to discuss those efforts.

If a business is subject to the CCPA, purchasers and investors should consider whether the target has appropriate mechanisms in place to comply with the law's obligations. The CCPA requires businesses to comply with certain consumer requests as well as affirmatively provide notice to consumers of their rights. Under the CCPA, consumers have a right to (i) request that a business disclose what categories of personal information it has collected, sold, or disclosed for a business purpose, (ii) request that a business delete any personal information collected from the consumer and (iii) opt out of the sale of the consumer's personal information.[14] Upon receipt of a verifiable request from a consumer, a business must take timely action to respond to the consumer's request and, if requested, provide disclosure, in writing, regarding the personal information collected, sold or disclosed for a business purpose in the preceding 12 months.[15]

Businesses subject to the CCPA are required to notify consumers of their rights under the CCPA in the business's privacy policy and in any California-specific notice regarding consumers' privacy rights.[16] Any business that collects, sells or discloses personal information for a business purpose must describe the categories of personal information collected, sold or disclosed in the privacy policy or notice.[17] A business cannot require that a consumer create an account with the business in order to receive the disclosure.[18] If a consumer requests that a business delete personal information regarding that consumer, a business

---

[13] *Id.* § 1798.140(t)(2).

[14] *Id.* §§ 1798.100-120.

[15] *Id.* § 1798.130(a)(2).

[16] *Id.* § 1798.130(a)(5).

[17] *Id.*

[18] *Id.* § 1798.135(a)(1).

must delete the personal information unless it is necessary for the business to, for example, perform a contract between the consumer and the business, detect security incidents, debug a product or perform other specific activities enumerated in the CCPA.[19]

- Practice Tip: Evaluate whether the target has sufficient procedures in place to evaluate and respond to bad faith consumer requests, including, but not limited to, bad actors requesting disclosure of another's personal information.
- Practice Tip: The obligation to delete personal information in response to a verifiable request from a consumer requires businesses to direct any service providers to delete the consumer's personal information from their records, unless an exception applies.[20] This type of cooperation should be built into the target's contracts with its service providers. If the target is a service provider and is not otherwise subject to the CCPA, the target may still have an obligation to respond to such requests and delete consumers' personal information, unless an exception applies.

The CCPA also requires that businesses that sell personal information comply with certain additional affirmative notice obligations unique to the CCPA, in addition to any requirements under the California Online Privacy Protection Act or other privacy frameworks.[21] Such businesses must provide a "clear and conspicuous link" on their homepage, titled "Do Not Sell My Personal Information," to allow consumers to opt out of the sale of the consumer's personal information.[22]

Finally, the CCPA requires that businesses implement and maintain reasonable security procedures to protect personal information held by the business.[23] Such procedures must be reasonable in light of the nature of the personal information.[24]

- Practice Tip: A target's operations may be constrained by upstream compliance issues. For instance, a business that buys personal information from a business subject to the CCPA is prohibited from selling that same information unless the consumer received explicit notice that such information could be sold, and was provided an opportunity to opt out of the sale of their personal information.[25] Consider whether the agreements that govern the target's acquisition of such personal information included appropriate warranties regarding compliance with the CCPA. Depending on the timing of the acquisition of personal information, it may be unlikely.
- Practice Tip: If the target does sell personal information, consider whether the business has adequate mechanisms to track consumer requests and separate databases of personal information. Following the processing of a consumer's opt-out request, a business may not request subsequent authorization to sell personal information for at least 12 months.

CCPA Penalties

Purchasers and investors should consider the risks of non-compliance with the CCPA. The CCPA provides a private right of action for consumers whose non-encrypted personal information is subject to

---

[19] *Id.* § 1798.105(c)-(d).

[20] *Id.* § 1798.105(c).

[21] *Id.* § 1798.135(a)-b); *see also* Cal. Bus. & Prof. § 22575.

[22] *Id.* § 1798.135(a).

[23] *Id.* § 1798.150(a).

[24] *Id.*

[25] *Id.* § 1798.115(d).

an unauthorized access or disclosure as a result of a business's failure to implement and maintain reasonable security practices.[26] Among other forms of relief, a plaintiff may seek to recover damages valued at the greater of actual damages or statutory damages, which range from $100 to $750 per consumer per incident depending on the nature of the violation and the defendant's assets, liabilities and net worth.[27] Businesses are entitled to a 30-day notice and cure period before a plaintiff can commence an individual or class action seeking statutory damages.[28] Senate Bill 561, introduced in February of this year, would expand the private right of action to allow a consumer to bring a civil action for damages arising from violations of any obligation under the CCPA, eliminate the 30-day notice-and-opportunity-to-cure requirement and eliminate the California Attorney General's obligation to provide guidance in response to requests.[29] While this bill has yet to be considered by the full California Legislature, if passed, it would greatly expand businesses' potential liability.[30] Lawsuits under the private right of action may be brought beginning on January 1, 2020.[31]

In addition to the threat of private litigation, the CCPA provides for enforcement by the California Attorney General for any violation of the CCPA.[32] Beginning on the earlier of July 1, 2020, or six months after the publication of the final regulations under the CCPA, the California Attorney General may bring actions for an injunction and civil penalties of up to $2,500 for each violation, or up to $7,500 for each intentional violation, after a 30-day notice and cure period.[33]

- Practice Tip: Investigate the target's mechanisms to process notices of violations from private plaintiffs and the California Attorney General. Additionally, consider the target's past handling of data breaches as an indication of the level of risk that the target presents.
- Practice Tip: Carefully evaluate the security measures in place to protect consumers' personal information and avoid unauthorized access to evaluate whether the measures meet industry standards for security.
- Practice Tip: Consider whether a target has plans to significantly reduce the total amount of personal information they hold or plan to collect in the future, which can reduce compliance risks.

The threat of private actions by individuals whose personal information is subject to an unauthorized access or disclosure is a serious risk for companies that experience a breach of personal information.

Valuation Considerations

If the CCPA applies to a potential target, consider (i) how consistent the valuation model is with the scope of the company's ability to use personal information it collects, (ii) the potential costs to bring the business

[26] *Id.*

[27] *Id.* § 1798.150(a)(2).

[28] *Id.* § 1798.150(b).

[29] California Consumer Privacy Act of 2018: Consumer Remedies, S.B. 561, § 1798.150(a)-(c); *see also id.* § 1798.155(a)-(b).

[30] *See* "New Amendment Would Significantly Expand Liability Under California Consumer Privacy Act," Feb. 28, 2019, Davis Polk Cyber Blog, **https://www.dpwcyberblog.com/2019/02/new-amendment-would-significantly-expand-liability-under-california-consumer-privacy-act/**.

[31] *E.g., id.* § 1798.150(a)(1).

[32] *Id.* § 1798.155(b).

[33] *Id.* § 1798.185(c); *see also id.* § 1798.155(b).

into compliance with the CCPA from an operational perspective and (iii) the reputational and financial risks associated with CCPA non-compliance.

The CCPA provides consumers with the ability to review and limit businesses' use of their personal information.[34] Consumers may opt out of the sale of their personal information and may request that businesses and service providers delete personal information previously collected or shared with these service providers.[35] If a purchaser's or investor's valuation model relies on the continued use of existing databases of personal information, the model should reflect the risk that a portion of California consumers may request the deletion of their personal information or may opt out of future collection. Purchasers and investors should also consider whether a target's operational model feasibly allows the business to stop selling or sharing data upon a consumer's request. Additionally, if a purchaser's valuation model anticipates a materially different or expanded use of the target's database of personal information, the purchaser may need to provide notice of the new practice to the target's consumers and that may prompt some consumers to opt out.[36]

- Practice Tip: Ensure that the risks of possible use restrictions are considered in financial models and assumptions and by appropriate legal and business teams during diligence.
- Practice Tip: CCPA compliance can affect the valuation of companies not directly covered by the CCPA. Consider whether a target's business model relies on the acquisition of personal information from California consumers, and whether a loss of access to that data would change a valuation model.

The implementation of certain IT security and operational measures prescribed by the CCPA, including those described above, may impose additional financial costs. For example, if a business has actual knowledge that consumers are under 16 years of age, it must affirmatively seek consent of the consumer (or the consumer's parent or guardian, if the business has actual knowledge that the consumer is under 13 years of age) to sell that consumer's personal information.[37] Businesses that operate services targeted at younger demographics may have actual knowledge that consumers using the service are under 16 years of age.[38] Under the CCPA, the business may need to implement more rigorous mechanisms to seek and document these consumers' consent (or, as needed, the consumer's parent's consent) to sell their personal information.[39] This would be in addition to the implementation of appropriate data protection measures and revised general consumer-facing notices. The total costs of such measures could be significant.

- Practice Tip: Consider the sufficiency of the target's systems to track and map its data inventory. The CCPA requires companies to provide disclosures with detail regarding categories of personal information collected, sold or disclosed for business purposes, as well as categories of third parties to which the personal information is sold or provided. Implementing a new or revised inventory to properly track and account for these categories may be costly.

---

[34] *E.g., id.* § 1798.110(a).

[35] *E.g., id.* § 1798.120(a).

[36] *Id.* § 1798.140(t)(2)(D).

[37] *Id.* § 1798.120(c).

[38] *Id.* § 1798.120(c).

[39] *Id.*

- Practice Tip: For sellers, be prepared to respond if the company is asked about any notices received for CCPA violations that were subsequently cured or about the company's security procedures to protect personal information.

A target's non-compliance with the CCPA may result in significant financial and reputational harm. As discussed above, the law provides for enforcement actions by the California Attorney General and the right for certain claims by private plaintiffs.[40] Given the high statutory damages available to private plaintiffs under the CCPA, private suits may not be easily dismissed for lack of standing. As a result, the CCPA poses an additional potential cost of data breaches beyond existing state, federal and international penalties associated with data breaches. A data breach, or a civil case alleging intentional violations of the CCPA, could also result in serious reputational harm.

Purchase Agreement Considerations

Prudent purchasers and investors will factor CCPA compliance into their purchase agreement structuring and risk allocation mechanisms. Particular care should be exercised to determine whether the transfer of any personal information qualifies as a transfer as part of a merger or acquisition that is exempt from the definition of a sale of personal information under the CCPA, to ensure that consumer opt-out requests do not prevent wholesale transfers of personal information. The CCPA appropriately makes exceptions for the most common transaction structures from the definition of a sale of personal information, but if parties are contemplating a unique transaction structure, careful attention should be paid to ensure the structure falls within the exception.[41]

Covenants may be appropriate to ensure a target's continued compliance or the development of a compliance program, or to require notification of any new breaches between signing and closing the transaction. Risk allocation provisions should also be thoughtfully negotiated to ensure appropriate excluded liability, representation and indemnity coverage. Representations regarding compliance with law are insufficient to fully address data privacy risks and should be expanded to cover industry standards and practices, and the existence and handling of data breaches. Representations to consider also include: (i) operation in accordance with the company's written privacy policy and contractual obligations, (ii) provision of all applicable privacy and cybersecurity policies, (iii) absence of written notices regarding related violations and investigations, (iv) existence of commercially reasonable information security and breach notification programs and (v) absence of data security breaches, loss of data and unauthorized disclosures of personal information.

Post-Transaction Considerations

The post-closing process of transferring and integrating data can last for up to several years, especially if the acquisition involves a business carve-out with related transitional services arrangements. During this period, either the seller or the purchaser may be required to continue providing data processing services for the other. In these cases, parties should consider structuring transitional services agreements to account for the CCPA. Specifically, the parties should include provisions (i) prohibiting the provider of service from (A) selling any personal information provided by the service recipient, (B) retaining, using or disclosing such personal information for any purpose other than performance of services and (C) retaining, using or disclosing the information outside of the direct business relationship between the parties and (ii) certifying that the provider of service understands those restrictions and will comply with them. Obtaining a representation from the provider of service that they will not misuse the personal

[40] *Id.* § 1798.155(b); *see also id.* § 1798.150(a).

[41] *Id.* § 1798.140(t)(2)(D).

information can also help buttress this argument.[42] Entering into this type of contract will also make the provider of service a "service provider" under the CCPA and so lessen the need for related notice and "right to opt-out" obligations. For businesses, including these types of contractual provisions, including covenants that prohibit the service provider from violating the CCPA, may help a business's ability to benefit from this carve-out.[43] A business is not liable for a service provider's violations of the CCPA so long as the business does not have actual knowledge or a reason to believe that the service provider intends to violate the CCPA at the time the personal information is transferred.[44] Companies should take care to properly establish restrictions and boundaries for the transfer and use of personal information in any transitional services arrangements.

As discussed above, a purchaser may also have an obligation to notify the target's consumers of any new use for previously collected personal information, if the new use is materially different from the target's prior use of the personal information.[45]

After the transaction, the purchaser should more rigorously evaluate the target's data security practices and breach notification processes, or integrate the acquired business into the purchaser's existing data security infrastructure. Purchasers and targets alike should consider whether voluntary changes in data privacy and data security practices are called for, even in the absence of CCPA compliance considerations. Other U.S. states are considering and enacting similar legislation, and federal privacy legislation may be soon to follow, so preemptive changes to personal information collection, storage, maintenance and deletion practices may be worthwhile investments.

- Practice Tip: Consider running cyber drills or tabletop exercises to test the combined company's or target's ability to respond to data breach incidents. These exercises may preemptively allow a purchaser to improve data security, and may provide additional documentation to assert reasonable security measures in the case of private actions under the CCPA.
- Practice Tip: In the post-closing process of integrating data, consider utilizing flexible databases to ensure more efficient compliance with amendments to the CCPA and future privacy legislation.

Conclusion

The CCPA is due to become effective January 1, 2020. Although the law currently provides for a six-month grace period for enforcement actions brought by the California Attorney General, prudent investors, purchasers and sellers are already working with their counsel to address a target's compliance with the CCPA and considering the implications for M&A transactions.[46] The requirements of the CCPA may impact all phases of a deal and should be taken into consideration from diligence through structuring to post-closing integration activities. Amendments to the bill have been put forward in the California Legislature, and the California Attorney General is authorized to continue to adopt regulations as necessary to further the purpose of the CCPA.[47] We will monitor and provide further updates as the CCPA becomes effective and enforcement actions begin.

---

[42] *Id.* § 1798.140(w)(A)-(B).

[43] *Id.* § 1798.140(t)(2)(C); *see also id.* § 1798.140(v).

[44] *Id.* § 1798.145(h).

[45] *Id.*

[46] *Id.* § 1798.185(c).

[47] *Id.* § 1798.185(b).

Davis Polk

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

Frank J. Azzopardi	212 450 6277	frank.azzopardi@davispolk.com
David R. Bauer	212 450 4995	david.bauer@davispolk.com
Avi Gesser	212 450 4181	avi.gesser@davispolk.com
Jon Leibowitz	202 962 7050	jon.leibowitz@davispolk.com
Pritesh P. Shah	212 450 4147	pritesh.shah@davispolk.com
Matthew J. Bacal	212 450 4790	matthew.bacal@davispolk.com
Daniel F. Forester	212 450 3072	daniel.forester@davispolk.com

Annex A: Sample Diligence Questions to Ask Potential Targets

- **Question: What portion of your annual revenues derive from the commercialization of personal information?**
  - Note: This is relevant because one of the ways a company becomes subject to the CCPA as a regulated business is if it (i) does business in California, (ii) collects, or directs others to collect, consumers' personal information and determines the purposes and means of processing of consumers' personal information and (iii) derives 50% or more of its annual revenues from selling consumers' personal information.
- **Question: What portion of personal information collected, sold or disclosed on an annual basis is collected from California residents or households?**
  - Note: This is relevant for two reasons. First, another way a company becomes subject to the CCPA as a regulated business is if it (i) does business in California, (ii) collects, or directs others to collect, consumers' personal information and determines the purposes and means of processing of consumers' personal information and (iii) annually buys, sells, or receives or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households or devices. Second, it is useful to consider the potential lost value if the target loses access to or the ability to commercialize personal information from California consumers.
- **Question: How is personal information stored and maintained?**
  - Note: This is relevant to assess how easily a target will be able to comply with the CCPA requirements to timely report on categories of personal information collected, sold or disclosed and timely delete personal information when requested.
- **Question: What security procedures and practices do you have in place to protect personal information?**
  - Note: This is relevant to assess the potential risk of private actions under the CCPA in the event of a data breach, as plaintiffs must allege that any disclosure of personal information occurred as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices.
- **Question: Do you rely on, purchase or otherwise receive personal information from third parties regarding California residents or households?**
  - Note: If the business relies on third-party data regarding California residents or households, and the individual exercises its right to opt-out of sales from the third party, that may prevent the data from being shared with the business and impact the business's commercial model.
- **Question: Do you provide data processing services for any businesses that may be subject to the CCPA?**
  - Note: This is relevant as businesses subject to the CCPA are obligated to direct service providers to delete personal information upon a verifiable request from a consumer to the business. While a service provider is not liable for the obligations of a business for which it provides services, a service provider may be liable for enforcement actions brought under the CCPA for its own violations of the law.

- **Question: Do your services target minors under the age of 16?**
  - Note: This is relevant as the CCPA imposes an obligation to affirmatively seek consent from a consumer (or that consumer's parent or guardian) to sell that consumer's personal information if the business has actual knowledge that the consumer is under 16 years of age (or 13 years of age). A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the age, and a company that targets minors may be more likely to be held to willfully disregard the consumer's age.