Cooley

cyber/data/privacy

California Consumer Privacy Act of 2018 (CCPA) Checklist

April 9, 2019

Contents

1. Introduction 1
2. What entities does the CCPA cover? 2
3. What information does the CCPA cover? 3
4. What activities does the CCPA cover? 5
5. What are the CCPA's exemptions? 6
6. What are the CCPA's privacy notice requirements? 8
7. What are the CCPA's consent requirements? 9
8. What are the CCPA's data security requirements? 10
9. What rights does the CCPA give Californians? 11
10. What are the CCPA's requirements for service providers and third parties? 14

1. Introduction

When it takes effect on January 1, 2020, the California Consumer Privacy Act of 2018 (CCPA) will have a sweeping effect on businesses in California and across the globe. The CCPA applies to a broad scope of information about California residents, and despite the law's name, not only when they act as consumers. Information about employees, job applicants, business contacts, students and other categories of individuals is also in scope, as is information about households and devices. As a result, the CCPA regulates an arguably broader scope of information than any other privacy law in the world.

The CCPA is enforced primarily by the California Attorney General, who may seek civil penalties of up to $2,500 per violation or $7,500 per intentional violation. However, the law also provides a private right of action for data breaches arising from violations of California's data security law, and entitles affected individuals to seek recovery of $100-$750 in statutory damages per consumer per incident or actual damages, whichever is greater.

The California legislature hastily passed the CCPA to preempt a more stringent November 2018 ballot measure. As a result, the 10,000-word law contains a number of drafting errors and ambiguous provisions. So called "technical amendments" enacted in September 2018 did little to resolve the law's ambiguities. The California Attorney General is required to issue regulations on numerous aspects of the CCPA by July 1, 2020, and cannot bring enforcement actions until it publishes the final regulations. While the regulations should offer clarity on some points and more amendments are possible, the CCPA's core provisions are expected to remain intact.

In any event, January 1, 2020 remains the compliance deadline and the effective date of the private right of action for data breaches. The breadth of the law and the potential difficulty of operationalizing its requirements create strong incentives to begin preparing for the CCPA sooner than later. This checklist provides an overview of the CCPA's core requirements, along with practical steps businesses can take to help comply, and can serve as a reference in performing preliminary gap assessments against the CCPA's requirements.

If you have questions or need assistance with the CCPA, please contact a member of Cooley's cyber/data/privacy team.

Mike Rhodes
San Francisco

+1 415 693 2181
rhodesmg@cooley.com
www.cooley.com/rhodesmg

Adam Connolly
San Francisco

+1 415 693 2111
aconnolly@cooley.com
www.cooley.com/aconnolly

Travis LeBlanc
San Francisco, DC
+1 415 693 2178
+1 202 728 7018
tleblanc@cooley.com
www.cooley.com/tleblanc

David Navetta
Denver

+1 720 566 4153
dnavetta@cooley.com
www.cooley.com/dnavetta

Boris Segalis
New York

+1 212 479 6610
bsegalis@cooley.com
www.cooley.com/bsegalis

2. What entities does the CCPA cover?

The CCPA addresses three categories of companies that handle personal information about California residents: businesses, service providers and third parties.

140(c)(1)[1]	**Business.** The CCPA's core provisions apply to "businesses". A business is defined as a for-profit legal entity that: • collects personal information of consumers ("**PI**"); • alone or jointly with others determines the purposes and means of processing of that PI; • does business in California; and • satisfies one or more of the following thresholds: 1. Has annual gross revenues greater than $25 million; 2. Annually buys, sells, or receives or shares for commercial purposes PI of at least 50,000 California residents, households or devices; or 3. Derives at least 50% of its annual revenue from selling California consumers' PI.	**Companies should** • Determine whether they or their affiliates do business in California, bearing in mind that "doing business in California" is broadly construed. • Determine whether those entities collect PI and satisfy any of the three thresholds, bearing in mind that even 50,000 annual unique visitors to a website from California can trigger the second threshold given the broad definition of PI. • For each entity that exceeds one of the thresholds, identify each of its affiliates with a shared name, servicemark or trademark, which will also form part of the business for CCPA purposes. • Determine whether the entities identified determine the purposes and means of processing the PI. This language was taken from the definition of a "controller" under the GDPR, and thus EU regulatory guidance on what constitutes a "controller" may be instructive on this question. • Determine whether they may also act as a service provider – a role analogous to the role of "processor" under the GDPR – by confirming whether the entity's contracts with the relevant businesses meet CCPA's requirements. If not, the entity is likely a third party.
140(c)(2)	Each affiliate that controls, is controlled by or is under common control with, the business and shares with the business "common branding" (i.e., name, servicemark or trademark) is also a business even if that affiliate itself does not trigger the thresholds.	
140(v)	**Service provider.** A service provider is a for-profit legal entity that processes information on behalf of a business and to which the business discloses a consumer's PI for a business purpose pursuant to a written contract. The contract must prohibit the service provider from retaining, using or disclosing PI for any purpose other than the specific purpose of performing the services required by the contract.	
140(w)	**Third party.** A third party is any individual or entity that is not a business or a service provider but receives PI from or on behalf of a business. It is important to note that a company can be a "business", "service provider" or "third party" in one context, and play another of these roles in another context. For example, a B2B service provider could be a business in relation to its website visitors, a service provider in relation to PI processed on behalf of its B2B customers, and a third party in relation to sales leads purchased from another business.	

[1] All citations in this document refer to subsections of Cal. Civ. Code § 1798.

3. What information does the CCPA cover?

The CCPA applies to the "personal information" of "consumers", encompassing a broad scope of information about any California resident.

140(o)	**Personal Information.** Personal information is defined as "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." The inclusion of *household* means that PI[2] can refer to multiple individuals (i.e., occupants of the same household). The definition also includes the following non-exhaustive examples of PI: • Real name, alias, signature, email address, phone number or postal address; • Driver's license or other state-issued identification number, social security number, passport number or similar identifiers; • Bank account number, credit card number, debit card number, insurance policy number or any other financial information; • Medical information, health insurance information, biometric information or physical characteristics or description; • Professional or employment-related information; • Education information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (FERPA); • Characteristics of protected classifications under California or federal law, such as race, national origin, color, ancestry, language, sex/gender, sexual orientation, marital status, age, medical condition, mental or physical disability, genetic information, religious creed, veteran/military status and status as a transitioning transgender person; • Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application or advertisement; • Account name, IP address, unique personal identifier or online identifier and geolocation data;	**Companies should** • Identify the categories of California residents with whom the company has contact, such as consumers, current and prospective customers, website/app users, employees, job applicants, and business contacts. • Identify the categories of California households with whom the company has contact (e.g., households served by internet-connected devices or household recipients of direct mail to "current resident"). • Determine whether the company handles any PI in connection with its relationships with the identified residents or households. • Consider expanding use of deidentified or aggregated consumer information to limit CCPA obligations. • Implement the safeguards and processes required by the definition of deidentified data to claim CCPA's exemptions for deidentified data, and consider implementing a deidentification standard or similar policies or procedures to demonstrate compliance with these requirements.

[2] As used in this checklist, "PI" refers to personal information of consumers (i.e., California residents).

	• Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies; and • Audio, electronic, visual, thermal, olfactory or similar information. PI also includes any inferences drawn from any of the above information to create a profile about a consumer reflecting the consumer's preferences, characteristics, preferences, behavior, abilities, intelligence or aptitudes. However, the CCPA does not restrict use of:	
140(a)	• **Aggregate consumer information** defined as "information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device".	

140(h)	• **Deidentified information** defined as "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:
	  • Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain;
	  • Has implemented business processes that specifically prohibit reidentification of the information;
	  • Has implemented business processes to prevent inadvertent release of deidentified information; and
	  • Makes no attempt to reidentify the information.	

140(g)	**Consumer.** Although the CCPA's title implies a consumer focus, the law broadly defines consumer as "a natural person who is a California resident . . . however identified, including by any unique identifier." As a result, consumers include not only B2C customers or prospects, but also employees, job applicants, business contacts, students, and other categories of individuals.	

4. What activities does the CCPA cover?

The CCPA's core requirements focus on collection of PI, and on sharing of PI in the form of a disclosure for a "business purpose" or a "sale".

140(e)	**Collection.** The CCPA defines collection as "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior." Note that this broad definition is triggered in any circumstance by which a business comes into possession of PI, which may include: • Collection directly from consumers; • Receipt of PI from other parties; and • Passive collection through server logs, cookies and other online tracking technologies that collect PI automatically.	**Companies should** • Analyze all disclosures of PI to determine whether they constitute "sales" or disclosures for business purposes, noting that most disclosures will likely constitute sales unless the recipient is subject to a contract that qualifies it as a service provider (See Section 1). • Prepare data maps documenting the collection, sale and disclosure of PI that will be needed to inform accurate disclosures in privacy notices and responses to consumers' information requests.
140(t)	**Sale.** Sales of PI are subject to the CCPA's more stringent transparency, consent and opt out requirements. The CCPA defines sale 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." Note that sales: • Do not require exchange of monetary consideration, such that any disclosure of PI for which something of value is received in return (e.g., freeware that requires processing of PI) would constitute a sale; • Do not include disclosures to service providers necessary to perform a business purpose, provided that the business has notified consumers of the disclosure and the service provider does not collect, sell or use the PI except as necessary for the business purpose; and • Do not include certain sales directed by consumers, sharing of identifiers incidental to alerting third parties of consumer opt out requests, and transfers in connection with M&A transactions and bankruptcy.	
140(d)	**Disclosure.** The CCPA distinguishes a disclosure for a business purpose from a sale. A disclosure of PI for a "business purpose" is not subject to the CCPA's consent and opt out requirements. The definition of "business purpose" generally refers to the business's or service provider's operational purposes and includes what appears to be an exhaustive list of seven activities that can constitute a business purpose: auditing, security, debugging, short-term transient use, performing services on the business's or service provider's behalf, internal research, and device safety and quality.	

5. What are the CCPA's exemptions?

The CCPA includes exemptions for information covered by certain other privacy laws and standards; M&A and bankruptcy; and commercial conduct wholly outside of California.

145(c)-(f)	**Information governed by other sectoral privacy laws and standards.** The CCPA has exemptions for certain information subject to: • Health Information Portability and Accountability Act (HIPAA); • California's Confidentiality of Medical Information Act (CMIA); • Fair Credit Reporting Act (FCRA); • Gramm Leach Bliley Act (GLBA); • California Financial Information Privacy Act (CFIPA); and • Driver's Privacy Protection Act (DPPA). The exemptions for GLBA and DPPA do not extend to the private right of action for security breaches. **Clinical trials.** The CCPA also exempts clinical trial information collected pursuant to the Common Rule, Good Clinical Practice guidelines, or FDA human subject protection regulations.	**Companies should** • Determine whether exemptions apply, noting that the exemptions citing other statutes will generally apply only to information regulated by that statute, and that CCPA regulates a broader scope of information. • Document their analysis supporting the conclusion that an exemption applies, which can demonstrate good governance and encourage leniency in an enforcement action concluding the exemption does not apply. • Analyze privacy policies and disclosures of any companies targeted for acquisition to determine whether the acquirer can freely use PI as contemplated, and assess their obligations to notify consumers of material changes to the use or sharing of PI.
140(t)(2)(D)	**M&A and bankruptcy.** Sales regulated by the CCPA do not include transfers to a third party of PI as part of a merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with the disclosures made to the consumers as required by the CCPA. To make material changes to the use or sharing of PI, businesses must give prior, prominent notice to the consumers that ensures they can easily exercise their CCPA opt out rights, and they must comply with other applicable restrictions under California's Unfair and Deceptive Practices Act (e.g., restrictions on material retroactive privacy policy changes).	
145(a)(6)	**Conduct wholly outside of California.** The CCPA exempts commercial conduct "if every aspect of that commercial conduct takes place wholly outside of California," meaning: • The business collected that information while the consumer was outside of California;	

	• No part of the sale of the consumer's personal information occurred in California; and • No personal information collected while the consumer was in California is sold.	
145(a)	**Legal obligations and proceedings.** The CCPA provides that it shall not restrict a business's ability to: • Comply with federal, state or local laws; • Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state or local authorities; • Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider or third party reasonably and in good faith believes may violate federal, state or local law; • Exercise or defend legal claims; and • Preserve legal privilege.	
145(k)	**First Amendment.** The CCPA provides that it does not apply to noncommercial activities of the press described in Article 1, Section 2(b) of the California Constitution.	

6. What are the CCPA's privacy notice requirements?

The CCPA substantially changes both the required contents and online presentation of privacy notices.

130(a)(5) 130(a)(1); 140(i) 100(b) 135	**Content requirements.** A business's privacy notice must disclose the following information and update it at least every 12 months: • The categories of PI the business has **collected** about consumers in the past 12 months; • The categories of PI the business has **sold** in the past 12 months; • The categories of PI that the business has **disclosed for a business purpose** in the past 12 months; • A description of the consumer's disclosure, access, opt out and nondiscrimination rights (detailed in Section 9); and • Two or more designated methods (i.e., mailing address, email address, web page, toll-free phone number or other contact info) by which consumers can submit requests to exercise their CCPA rights. These methods must include a toll-free phone number and a web address if the business has a website. **Presentation requirements.** At or before the point of collection of PI, a business must inform consumers of the categories of PI to be collected and the purposes for which each category of PI will be used. While not expressly required, setting out this information in a privacy notice linked at the point of collection will be a natural way to provide this information. The business must create a webpage titled "Do Not Sell My Personal Information" that enables a consumer to opt out of the sale of his or her PI. The business must provide a link to this webpage: • On the business's homepage (or a separate homepage dedicated to California consumers); • In its online privacy policy; and • In any California-specific description of consumers' privacy rights.	**Companies should** • Prepare data maps documenting the company's collection, sale and disclosure of PI, which will be needed to inform accurate disclosures in privacy notices and responses to consumers' information requests. • Update privacy notices to include the disclosures required under the CCPA by January 1, 2020.[3] • Note that privacy notices posted on January 1, 2020 will need to describe activity in 2019 under the 12 month "look back". • Update privacy notices at least every 12 months. • Provide separate CCPA-compliant privacy notices to California employees, job applicants, and any other categories of consumers to whom the business's website is not directed. • Carefully structure "globalized" privacy notices to address the CCPA and other global privacy laws (e.g. GDPR) in a manner that avoids unintentionally availing individuals of rights to which they are not legally entitled (for example, EU residents are not entitled to CCPA rights and Californians may not be entitled to GDPR rights). • Update website terms of service to ensure consistency with updated privacy notices.

[3] Publishing the privacy notice update before January to give consumers prior notice 1 (e.g., 30 days) would be consistent with best practice, but the updated privacy notice should clarify that it will not take effect until January 1, 2020, or it will avail Californians of rights (see Section 9) that they do not yet have.

7. What are the CCPA's consent requirements?

The CCPA is not a consent-based framework – it focuses on transparency and the right to opt out – but does require consent to sell PI of minors and to enter consumers in rewards or other financial incentive programs.

120(c) 125(b)(3)	**Minors.** A business may not sell PI of a consumer if it has actual knowledge that the consumer is under 16 years of age unless the sale was affirmatively authorized by: • The consumer, if the consumer is 13-15 years of age; or • The consumer's parent or guardian, if the consumer is under 13. Willful disregard of the consumer's age is deemed actual knowledge of it. **Financial incentive programs.** A business may enter a consumer into a financial incentive program only if the consumer gives the business the notices required by CCPA, as well as a description of the material terms of the financial incentive program, and obtains the consumer's prior opt-in consent. The consent is revocable by the consumer at any time. The CCPA does not define financial incentive program but states that "[a] business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information." Such offers would fall within the consent requirement. Rewards programs would be a common example.	**Companies should** • Determine whether they have actual knowledge that they sell PI of minors under 16. • Determine the risk of being charged with willful disregard of consumers' ages and consider age screening and consent mechanisms to limit risk where appropriate. • Implement consent or parental consent mechanisms as necessary to authorize selling PI of minors under 16. • Ensure rewards and other financial incentive programs provide CCPA-compliant privacy notices and require the consumer's informed, prior consent after presenting the program's material terms. • Pending clarification or guidance on these issues under CCPA, consult the Federal Trade Commission's guidance under the Children's Online Privacy Protection Act (COPPA) on what constitutes valid parental consent, appropriate age-screening techniques, and when a site is deemed directed at children such that age screening and consent mechanisms are required.

8. What are the CCPA's data security requirements?

The CCPA does not directly impose data security requirements but creates a private right of action for data breaches arising from failure to maintain reasonable security as required by California's data security law.

150	**California's data security law.** California Civil Code 1798.81.5 requires a business that owns, licenses or maintains certain categories of personal information about a California resident to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."
	The categories of personal information subject to this requirement are:
	• An individual's first name or first initial and last name in combination with any one or more of the following data elements, when not encrypted or redacted:
	  • Social security number;
	  • Driver's license number or California identification card number;
	  • Account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account;
	  • Medical information; or
	  • Health insurance information; or
	• A username or email address in combination with a password or security question and answer that would permit access to an online account.
	CCPA's private right of action. The CCPA provides that if unauthorized access and exfiltration, theft or disclosure of this information results from the business's violation of its duty to implement and maintain such reasonable security procedures and practices, the affected consumers may institute a civil action to recover statutory damages of $100-$750 per consumer per incident or actual damages, whichever is greater. Affected consumers may also seek injunctive, declaratory relief or other relief the court deems proper.
		Companies should
		• Implement a written information security program that employs reasonable physical, technical and administrative controls designed to protect PI. The controls should ideally be aligned with a recognized information security control framework (for example, the California Attorney General issued non-binding guidance in 2016 that "reasonable security" requires implementation of the Center for Internet Security Critical Security Controls[4]).
		• Implement an incident response plan and conduct incident response simulations to prepare to effectively respond to a security incident.
		• Implement a vendor risk management program, including procedures for exercising security oversight over service providers that handle PI and ensuring that contracts with service providers contain appropriate security requirements.

[4] California Data Breach Report, February 2016, available at https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

9. What rights does the CCPA give Californians?

Businesses must honor Californians' rights to information about the collection, use, sale and disclosure of their PI, to access and delete their PI, and to opt out of the sale of their PI. Californians have the right to exercise these rights free from discrimination.

130(a)(2) 145(g)(1)	**Honoring individual rights.** When businesses receive requests to exercise individual rights under CCPA, they must verify the requests and comply with them within 45 days of the request (which may be extended for "up to 90 additional days where necessary, taking into account the complexity and number of the requests").	**Companies should** • Prepare data maps documenting the collection, sale and disclosure of PI that will be needed to inform accurate disclosures in privacy notices and responses to consumers' information requests. • Ensure applications and IT systems are designed to accommodate compliance with individuals' requests without adverse effects on systems or processes. This is often one of the costliest compliance efforts due to the difficulty of meeting these requirements with legacy systems not designed with these requests in mind. • Implement procedures and technical capabilities for verifying the identities of individuals making requests in accordance with California AG regulations, once issued. • Consider building capabilities to automate compliance with these requests to reduce associated manual effort and cost-to-serve. • Implement internal policies and procedures designed to help relevant personnel recognize, triage and execute on individual requests (and differentiate them from GDPR data subject requests). • Implement procedures and contractual rights necessary to direct service providers to assist with compliance with individuals' requests to exercise their rights as it relates to PI that service providers hold. • Consider how high volumes of requests to opt out of the sale of PI would business models that rely
130(a)	Businesses must make a designated method available for exercising individual rights, including a toll-free phone number and a web page that consumers can use to exercise their rights to information about and access their PI.	
130(a)(6); 135(a)(3)	Businesses must ensure that all personnel responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA are informed of the business's obligations to honor individual rights and how to direct consumers to exercise them.	
140(y)	Businesses must verify the identities of consumers making requests to exercise their CCPA rights.	
192	Terms of agreements with consumers purporting to waive their CCPA rights are void and unenforceable.	
100, 110	**Right to access PI.** Businesses must honor Californians' requests to access their PI, and if provided electronically, provide the PI in a portable format that allows transfer to another entity. Businesses do not need to honor this request from the same requester more than once every 12 months.	
105	**Right to delete PI.** Businesses must honor Californians' requests to delete their PI and direct its service providers to do the same, unless the business needs the PI to: • Provide a good or service requested by the consumer; • Provide a good or service reasonably anticipated within the context of a business's ongoing relationship with the consumer; • Perform a contract with the consumer; • Detect security incidents or malicious or illegal activity; • Debug or repair existing intended functionality; • Exercise, or allow the consumer to exercise, free speech or another legal right;	

	• Enable internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business; • Engage in certain scientific research; • Comply with a legal obligation; or • Use the PI internally in a lawful manner compatible with the context in which the consumer provided it.	on PI sales (e.g., ad-supported free services and data brokerage). • Consider whether California-specific sites, products or services should be offered if applying the CCPA's protections to all users is too burdensome. • Train consumer-facing personnel to recognize requests to exercise individual rights and direct the requesters on how to make their requests. • Implement measures to prevent soliciting consumers to opt-in to the sale of their PI if they opted out in the past 12 months. • Include savings clauses in class action waivers and arbitration clauses in consumer-facing agreements in case they are challenged as invalid under CCPA.
130(a)	**Right to information about collection, sale and disclosure of PI.** Upon request, businesses must provide consumers with the following information for the 12 month period preceding the request: • The categories of PI it has collected about that consumer; • The categories of sources from which the PI is collected; • The business or commercial purpose for collecting or selling PI; • The categories of PI that the business sold about the consumer; • The categories of third parties to whom the PI was sold, organized by category of PI for each third party; • The categories of PI that the business disclosed about the consumer for a business purpose; and • The categories of third parties to whom the PI was disclosed for a business purpose, organized by category of PI for each third party.	
120	**Right to opt out of sale of PI.** A consumer may opt out of a business's sale of the consumer's PI, and may authorize another person or entity to opt out on the consumer's behalf. If a consumer has opted-out of the sale of the consumer's PI, a business must wait 12 months before requesting the consumer to re-authorize sale of the PI.	
125	**Right to nondiscrimination.** A business must not discriminate against a consumer (e.g., denying service, increasing price or decreasing service quality) because the consumer has exercised any rights under the CCPA. However, the CCPA provides that a business can charge a different price for or provide a different level or quality of goods or services to the consumer if that difference is reasonably related to the value	

	provided to the consumer[5] by the consumer's data. A business is permitted to offer financial incentives to consumers for the collection of PI, so long as: • The business notifies consumers of such financial incentives in its privacy policy and California-specific description of consumers' privacy rights; • The material terms of such financial incentives are clearly described to the consumer and the consumer provides prior opt-in consent, which is revocable at any time; and • The financial incentives are not unjust, unreasonable, coercive or usurious. The CCPA's seemingly conflicting nondiscrimination provisions are among those most in need of clarification, as they make the difference between discriminatory and permissible differences in price, service or incentives difficult to discern.	

[5] The current version of the CCPA states a different price can be charged or a different level of quality can be provided "if that difference is reasonably related to the value provided to the consumer by the consumer's data." (125(a)(2), emph. added.) However, it is possible this is a drafting error and the intent was to refer to value provided to the business, rather than to the consumer.

10. What are the CCPA's requirements for service providers and third parties?

The CCPA focuses its requirements on businesses, but service providers and third parties also face potential CCPA liability.

155(b) 140(w)(2)(B) 145(h)	**Service providers.** The CCPA contemplates that service providers may violate the CCPA and provides that they are liable for such violations, yet does not expressly impose obligations directly on service providers. The CCPA provides that businesses are not liable for service providers' use of PI in violation of the CCPA so long as they had no reason to believe the violation was intentional. Similarly, that service providers are not liable for the obligations of businesses for which they provide services. While the CCPA is unclear as to how service providers can violate the law when it does not impose explicit obligations on them, service providers should ensure their contracts with businesses contain the necessary limits on PI use to ensure they meet the definition of "service provider" and are not classified as businesses or third parties. Complying with those contracts is perhaps the best way for service providers to minimize the risk of CCPA-related liability.	**Companies should** • Identify the contexts in which they act as service providers or third parties. • Ensure contracts with service providers meet the requirements of a service provider contract and allocate CCPA liability appropriately. • Consider drafting contracts with business partners to support the position that the business partner is not a third party for CCPA purposes and/or that the disclosure of PI to the business partner is not a "sale" under CCPA.
115(d)	**Third parties.** CCPA imposes only one obligation directly on third parties, namely, that a third party "shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out." It is important to note that a company can be a "business", "service provider" or "third party" in one context, and play another of these roles in another context. For example, a B2B service provider could be a business in relation to its website visitors, a service provider in relation to PI processed on behalf of its B2B customers, and a third party in relation to sales leads purchased from another business.	• Consider whether any sharing of PI would trigger CCPA's restrictions on sales by third parties and how the third party seller can comply with CCPA's explicit notice obligations even where it has no direct relationship with the relevant consumers. More broadly, companies with business models that rely on sales or resales of PI should consider the impact of CCPA's third party sale restrictions on these business models and whether CCPA liability and compliance obligations can be contractually allocated their counterparties in these transactions to an acceptable degree.

For more information, follow our blog at **https://cdp.cooley.com/tag/ccpa/**