Negotiating with Service Providers and Third Parties under CCPA

Tanya Forsheit, CIPP/US, CIPT
Partner and Chair, Privacy & Data Security Group,
Frankfurt Kurnit Klein & Selz

KEY TAKEAWAYS

- *Contractual provisions that address GDPR requirements will not necessarily cover CCPA requirements.*
- *Third parties are entities that are not envisioned under the GDPR.*
- *"Service provider" relationships require strict contractual restrictions on what the vendor can do with the information.*
- *Any exchange of personal information that is not accompanied by the contractual restrictions required to meet the definition of "service provider" — or what is not a "third party" — is at risk of being found to be a "sale" if there is valuable consideration involved.*
- *There are emerging industry proposed solutions that may help address some of the contractual complexities raised by the CCPA.*

Introduction

Many of us understand in theory what the California Consumer Privacy Act means for consumer rights and that it creates a totally new ecosystem of relationships between and among businesses that are covered by the law and other legal entities with whom they do business.

Unfortunately, that new ecosystem bears little resemblance to the controller/processor structure of the EU General Data Protection Regulation and leaves much to be desired when it comes to facilitating the privacy practitioner's job of categorizing and risk-ranking business partners. To make matters worse, the attorney general did not issue draft regulations until October, and those regulations likely will not be finalized until July of 2020.

This white paper is designed to provide a little guidance to those who are struggling to identify different parties in the ecosystem and draft contractual provisions accordingly. It is also intended to become a chapter in the second edition of the IAPP's "Data Processing Agreements" book in 2020.

This white paper is not legal advice. Readers should retain counsel to advise them on privacy practices and contract negotiations/drafting. As the CCPA evolves, moreover, please consult more recent versions of this paper or other updated materials in the IAPP Resource Center.

Definitions of business/service provider/third party under CCPA

The definitions section of the CCPA is primarily found in Civil Code Section 1798.140. The first key definition is "business." What is a covered "business" for purposes of the CCPA?

Section 1798.140(c) defines a "business" as:

> (1) A sole proprietorship, partnership, limited liability company, corporation, association or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:
>
>> (A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.
>>
>> (B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households or devices.
>>
>> (C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.
>
> (2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark or trademark.

If you meet the definition of a business, the next step is to determine what your business partners and vendors are in the CCPA landscape. Even if you are not a "business," you may receive inquiries from companies that are "businesses" as to what role you play. Accordingly, the next most relevant definition is "service provider."

Section 1798.140 (v) defines a "[s]ervice provider" to mean:

> [A] sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

But what if you are neither a business nor a service provider? Or what if you are doing business with companies that are doing things with the personal information you make available to them in ways that are not strictly for the purpose of providing services to you? The next definition we consider is "third party."

Section 1798.140(w) defines a "[t]hird party" by virtue of what it is not. A "third party" means a person who is not any of the following:

> (1) The business that collects personal information from consumers under this title.
>
> (2) (A) A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:
>
>> (i) Prohibits the person receiving the personal information from:
>>
>>> (I) Selling the personal information.
>>>
>>> (II) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.
>>>
>>> (III) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.
>>
>> (ii) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

> (B) A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.

If you feel like the definition of what is not a “third party” seems awfully similar but slightly different from what is defined as a “service provider,” you are right. It is just one example of the poor drafting of the CCPA.

Examples of business-service provider relationships

Given the poorly crafted definitions, how can a business know what to look for in determining whether its partners are “service providers”? Let’s consider some examples.

The most straightforward example of a business-service provider relationship is likely to be something like cloud hosting. If a cloud services provider is doing nothing with the data other than hosting (e.g., infrastructure as a service), the cloud services provider is a service provider for CCPA purposes. Another example would be a customer relationship management service that does not use the data for any purpose of than to provide the service.

That being said, neither of these kinds of companies (or any other) can be a service provider unless the contract includes the restrictions set forth in the section above. It is, therefore, best to use the definition of what a “third party” is not to help design your contract in a way that demonstrates your business partner is a service provider.

The bottom line: If you do not need your partner to use data in ways beyond providing you with the services or if you are a vendor that just provides a service (e.g., security services) and does nothing else with the data, draft a strong “service provider” agreement and be done with it.

Sample contract language

The “service provider” is the easiest language to draft because you can follow the statutory requirements in the definition of what is not a “third party” in Section 1798.140(w). Here is one way to approach it:

> [Company] is a Business and [Vendor] is a Service Provider for purposes of the CCPA. [Vendor] shall not: (a) sell the Personal Information; (b) retain, use or disclose the Personal Information for any purpose other than for the specific purpose of performing the Services; (c) retain, use, or disclose the Personal Information for a commercial purpose other than providing the

> Services; or (d) retain, use, or disclose the Personal Information outside of the direct business relationship between [Vendor] and [Company]. [Vendor] certifies that it understands these restrictions and will comply with them.

A word of caution: Don't try to shoehorn your vendor relationship into this model if it is not factually accurate. That can only end badly – like with an FTC Section 5 investigation.

Examples of business–third-party relationships

Now that we know what a "service provider" is, it is not difficult to determine what a "third party" is because (as mentioned above) "third party" is defined by virtue of what it is not — i.e., not a service provider. Any vendor doing anything with personal information other than providing the service (e.g., using the personal information for its own purposes) could be a "third party." Stated another way, any entity is a "third party" when the contractual restrictions described in the model contractual language above are not employed.

It also likely applies in any situation when a vendor has contractual language that allows it to use personal information to improve its services, engage in benchmarking, or allow other businesses to use the personal information.

"Third party" has no analog in the GDPR model; you may find many companies taking the position that they are "third parties" and/or independent "businesses," similar to the "independent controller" role under the GDPR, defining themselves as businesses (controllers) that make decisions about the purposes and means of processing.

Sample contract language

> The following sample clauses are premised on the assumption that the "third party" will also take the position that it is an independent "business," much like an independent controller for GDPR purposes.
>
> You will notice right away that the "third-party" model is much more complicated than the "service provider" model. This is because the law itself does not necessarily accommodate all the many business models (e.g., fraud prevention, advertising technology) that require the vendor to build its own databases and use its own algorithms.
>
> For efficiency, this sample includes GDPR terminology, but users should remove it if not relevant to the situation.

1. **Sample language for parties' roles/data ownership as to 'business data' and 'vendor data'**

Sample language for data license of business data to vendor (this imposes restrictions similar to the "service provider" language discussed above, to allow the business to take the position that, as to business data, it is a business and the vendor is the "service provider"):

The parties acknowledge that, as between Business and Vendor, all Business Data that is subject to the Agreement is owned by the Business. The Business retains all right, title and interest in Business Data, and any rights not expressly granted herein are reserved by the Business. The Business acts as a Controller and Business of the Business Data. Vendor shall act as a Processor and Service Provider of the Business Data it processes under the Agreement. The Business, as a Controller/Business, determines the purposes and means of the processing of the Business Data.

[Note: How "business data" is defined will depend in large part on the services involved, but it should incorporate a definition of "personal data/ information." The business data should include the personal information the vendor only gets from the business and no one else and only uses for the business and for no other purpose.]

The Business hereby grants to Vendor a limited, revocable, non-exclusive, royalty-free right and license during the term of the Agreement to Process Business Data for the sole purpose of providing the Services and for the purposes set forth in this Agreement. Vendor does not have any right to directly or indirectly sell, rent, lease, copy, access, use, combine, reproduce, modify, disclose or transfer Business Data, other than as set forth in this Agreement. Vendor shall not collect through the Business Properties any data from Users of Business Properties or use any such data, except as may be mutually agreed upon by the parties. Vendor shall not: (a) sell the Business Data; (b) retain, use, or disclose the Business Data for any purpose other than for the specific purpose of performing the Services; (c) retain, use, or disclose the Business Data for a commercial purpose other than providing the Services; or (d) retain, use, or disclose the Business Data outside of the direct business relationship between Vendor and the Business. Vendor certifies that it understands these restrictions and will comply with them.

For vendor data, consider something like the following:

Vendor owns Vendor Data that is subject to the Agreement. The parties agree that, unless otherwise agreed between the parties, both Vendor and the Business will be considered Controllers and Businesses of Vendor Data and all other Personal Information, other than the Business Data, processed in relation to the Services performed by Vendor pursuant to the Agreement.

[Note: How "vendor data" is defined will also be driven by the nature of the services and should also incorporate a definition of personal data/information. Vendor data should include the personal information that vendor gets from the business that vendor incorporates into its own database/service in order to provide the services.]

[Add GDPR language as appropriate]: Each Controller is responsible for Processing Personal Data in accordance with an appropriate lawful basis.

Notwithstanding anything to the contrary herein, in no event will Vendor and the Business be deemed to be jointly processing Business Data or Vendor Data. [Note: This should be revised if it is a joint controllership for GDPR purposes.]

Third-Party Data will remain the sole and exclusive property of such third parties and subject to their applicable license terms. [Note: This is important if the business or the vendor are also collecting/processing personal information from third parties.]

2. Sample provision to address consumer requests

Each party shall notify the other party of an individual within its organization authorized to respond from time to time to inquiries regarding the Business Data and Vendor Data including but not limited to data subject and consumer requests for deletion, disclosure and "Do Not Sell," and shall deal with such inquiries promptly, without prejudice to the specific deadlines imposed by Applicable Data Protection Law.

3. Sample language that can be used to address each party's compliance obligations

Each party shall only use or otherwise Process Personal Information in accordance with the permitted purposes set forth in this Agreement and in accordance with all Applicable Data Protection Law. Each party shall be individually and separately responsible for complying with the obligations under Applicable Data Protection Law that applies to it as a Controller or Processor, as applicable, in respect of certain types of Personal Information processed under the Agreement. Neither party shall share, transfer, disclose or otherwise provide or permit access to the Personal Information to any person or entity without the other party's prior written consent, except in accordance with this Agreement, or on the basis of a court order, subpoena, or other governmental requirement or authority, or in case such party is otherwise required to disclose such information by law or regulation, provided that such disclosure is permitted by Applicable Data Protection Law (a "Compulsory Request"). In such case, the disclosing party shall inform the other party of that legal requirement to disclose information before processing the Compulsory Request, unless applicable law prohibits such disclosure.

4. **Sample language for security safeguards and breach response**

   Each party shall implement and maintain (and require its Subprocessors to maintain) reasonable and appropriate technical, administrative and organizational measures designed to ensure a level of confidentiality and security appropriate to the risks represented by the processing and the nature of the Personal Information and to prevent unauthorized or unlawful processing of Personal Information, including but not limited to measures against accidental loss, disclosure or destruction of, or damage to, Personal Information. Each party agrees to notify the other party within a reasonable period of time (and in any event within forty-eight (48) hours) where such party becomes aware of or reasonably suspects that Personal Information of the other Party has been or may have been lost, damaged or subject to unauthorized internal or external access or any other unlawful processing (a "Security Incident") and to take reasonable steps to mitigate the impact of any such Security Incident. To the extent a party, as Controller/Business with respect to Personal Information subject to a Security Incident, seeks the assistance of the other party, the other party agrees to reasonably cooperate with such party to: (a) determine the scope and severity of any such Security Incident; (b) provide timely information and cooperation as such party may require to fulfill such party's data breach reporting obligations under Applicable Laws and contract; and (c) give notice to individuals whose Personal Information is the subject of such Security Incident. Unless a party is obliged to give such notice under Applicable Data Protection Law, such party shall not give notice to individuals in respect of a Security Incident relating to Data of the other party except with the prior written approval of the other party.

5. **Sample language for deidentification. The CCPA also provides certain exemptions for information that is deidentified, so consider the following language if that is relevant and you believe you can meet the high bar for deidentification**

   If either party receives information of the other party in Deidentified format, such party shall: (1) implement technical safeguards that prohibit reidentification of the data subject or consumer to whom the information may pertain; (2) implement business processes that specifically prohibit reidentification of the information; (3) implement business processes that prevent inadvertent release of deidentified information; (4) not attempt to reverse engineer the information or otherwise reidentify data subjects or consumers to whom the Deidentified Data relates; and (5) only share the Deidentified Data, if and to the extent such sharing is permitted by this Agreement, in the format it received it from the other party. If a Party does not receive Personal Information in Deidentified format, but the other party instructs such party to only share Personal Information of the other party in a Deidentified format, such party shall ensure it is Deidentified before it is shared.

When might a vendor also be a 'business'?

As noted above, most situations in which a vendor is a third party will also involve the vendor being an independent business. This is very much like independent controller relationships under the GDPR. As one potential example, if an adtech provider refuses to restrict its use of personal information to the purposes set forth in the definition of a service provider, it will, by definition, be a third party and potentially also an independent business. This is what happened under the GDPR — most adtech providers refused to be processors and took the position that they are independent controllers. Interestingly, as we go to press, some adtech companies that took the position that they were independent controllers for GDPR purposes are now asserting that they are merely service providers for CCPA purposes. It will be interesting to see how they reconcile those legal positions.

A. Issues/potential contract language for the purchasing party/vendor?

The most significant consequence of a vendor refusing to be a service provider is that the CCPA considers nearly any exchange of information between a business and another entity other than a service provider (subject to the appropriate contractual restrictions described above) to be a "sale."

Any exchange of personal information is a "sale" if the business receives "monetary or other valuable consideration," unless an exception applies. Section 1798.140 (t)(1) defines "[s]ell," "selling," "sale" or "sold," 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."

Given how easily what you thought was a "service provider" relationship could become a "sale," it becomes extremely important to examine the enumerated exceptions to "sale."

Section 1798.140(t)(2) enumerates the exceptions as follows:

> For purposes of this title, a business does not sell personal information when:
>
> (A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

This first exception appears to indicate that, in the event a consumer explicitly consents (consistent with the GDPR's consent standard) to use of the personal information, that the disclosure at issue is not a sale. This might be a reason for businesses to consider using a cookie consent mechanism that they use for GDPR purposes for the CCPA, as well.

> (B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.
>
> (C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:
>
>> (i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.
>>
>> (ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

This exemption in subsection Section 1798.140(t)(2)(C) is simply a reiteration of the service provider exception discussed above. But it also requires us to look at the definition of "business purpose." Section 17980.140 (d) defines "business purpose" as:

> The use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are:
>
>> (1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.
>>
>> (2) Detecting security incidents, protecting against malicious, deceptive, fraudulent or illegal activity, and prosecuting those responsible for that activity.
>>
>> (3) Debugging to identify and repair errors that impair existing intended functionality.

> (4) Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.
>
> (5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.
>
> (6) Undertaking internal research for technological development and demonstration.
>
> (7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

Another important exemption from "sale" is in the event of a merger, acquisition, or other corporate reorganization.

Section 1798.140(t)(2)(D) exempts from the definition of sale situations where:

> The business transfers to a third party the personal information of a consumer 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, provided that information is used or shared consistently with Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

The most important takeaway is that any relationship that does not qualify as a "service provider" relationship because it lacks the contractual restrictions described above could be found to be a "sale" if there is valuable consideration involved.

Potential IAB Industry Solution

On Sept. 17, 2019, the Interactive Advertising Bureau rolled out a proposed CCPA Industry Framework to provide companies with a way to communicate through the digital advertising ecosystem certain information, including when a consumer exercises his or her right to opt-out of sale under the CCPA. The proposed IAB Framework includes an industry-wide contract to implement the rights and obligations triggered by the opt-out signal. This agreement would impose on the downstream participants the statutory limitations of a service provider in connection with the transactions in which they are involved that include the opt-out signal. These participants become "limited service providers," prohibited from selling personal information but still permitted to use the personal information to, for example, supplement a bid request and engage in bid decisioning to complete the transaction. The limited service provider would not, however, be able to use the personal information to build a new behavioral profile or augment a previously existing profile. Just prior to this paper going to press, on Nov. 18, 2019, the IAB issued a draft Limited Service Provider Contract.

The proposed Limited Service Provider Contract would eliminate the need for individual agreements among participants and solve for the issue of privity among participants who would not otherwise contract with each other (e.g., publishers and buy-side ad servers). An industrywide agreement also solves for the "onward sale" issue because it designates all downstream participants as service providers of the publisher, even without a direct relationship.

Organizations in the adtech ecosystem (including publishers, advertisers, agencies and adtech companies) will need to decide, working with their own legal counsel, whether it makes sense for them to sign on to the IAB Limited Service Provider Contract to address personal information exchanges for interest-based advertising (and the related consequences in the event of a "Do Not Sell" command) or, alternatively, to develop and enter into individual contracts with each of the other relevant players in the ecosystem.

Conclusion

Characterizing business partners and vendors as "service providers" or "third parties" is crucial to CCPA compliance. Existing contracts may need to be modified with a CCPA addendum addressing the parties' CCPA status and obligations. New contracts will also need to include CCPA-related language, and vendors should begin updating their standard forms now to capture concerns their business-to-business customers will undoubtedly raise and define themselves as a business provider (or third party) as appropriate.

Of course, the factual reality of the business relationship will ultimately determine whether an entity is a "service provider" or "third party" under the CCPA; that being said, the parties can assist in allocating risk and responsibility — if not determining legal status — by how they characterize themselves and their duties in their agreements.