CCPA Enforcement Area No. 3

Service Providers

Organizations that qualify as a "service provider" under the CCPA breathed a sigh of relief when realizing that most obligations imposed by the CCPA apply directly to "businesses." This includes, for example, providing the required notices (*i.e.*, Notice at Collection, Privacy Notice, Notice of Right to Opt Out, and Notice of Financial Incentive), implementing the "Do Not Sell" link, and offering methods for consumers to submit access, deletion, and opt-out requests. Of course, this does not mean the CCPA's sweeping compliance obligations left service providers free from regulation.

To qualify as service providers, organizations must agree in the data sharing contract to process personal information on behalf of covered businesses solely for the purpose outlined in the contract and further agree not to retain, use, or disclose the personal information for any other purpose. Service providers also likely agree to many compliance processes to assist such businesses with meeting their obligations under the law. From a practical perspective, this means that while service providers may not have visible flags of CCPA-compliance on their websites or external-facing materials, compliance exists behind-the-scenes and should be appropriately documented through updated contractual provisions and robust policies and procedures. This is particularly important given that it would not be surprising to see OAG send "notice and cure" letters to organizations that *appear* to have ignored the requirements of the law, even though such organizations are acting as service providers and thus exempt from many of the CCPA's requirements.

In light of restrictions included in the data sharing contracts, service providers should routinely assess their operations to ensure that they do not behave in a manner or use downstream customer data (sent by "businesses" under the CCPA) in a manner that is in contravention of their service provider role. Indeed, any investigation of, or enforcement action against, a "business" could implicate service providers who have downstream access to customer data—especially where data use is not limited to a "specific purpose." To avoid the risk of the OAG suspecting unfair and deceptive trade practices by organizations falsely claiming to be service providers or improperly disclosing data practices, service providers should be prepared to explain why they have customer data and why their use of that data is proper.

Troutman Pepper tips

- **Review Vendor Contracts**

  To qualify as service providers, organizations must update their vendor contracts to include the conditions and limitations imposed by the CCPA. This includes, for example, identifying the nature and purpose of processing personal information on behalf of the business and prohibiting the service provider from retaining, using or disclosing the personal information for any purpose other than the specified purpose.[1] As with most of the CCPA's requirements, there are certain exceptions to the processing restrictions. For example, § 999.314 of the final text of the proposed regulations provides that service providers may use personal information "to detect data security incidents, or protect against fraudulent or illegal activity" or for "internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source." Despite the fact the CCPA allows for this type of processing by a service provider, it should still be expressly called out in the vendor contract. Failure to do so may limit the service provider in how it can use the personal information despite the allowance afforded by the CCPA. Service providers also need to ensure that a strong contract management system has been implemented. Because service providers likely "service" more than just one customer, keeping track of the various (and perhaps conflicting) purposes permitted by the data sharing agreements will be critical.

[1] For additional information about updating vendor contracts in light of the CCPA, see our *Law360* article titled, *California Privacy Law Means New Approach to Vendor Contracts*, available here.

- **Be Prepared to Explain Your Organization's Position**

  If a service provider receives a "notice and cure" letter from the OAG, the service provider should be prepared to explain how it reached the conclusion that it qualifies as a service provider under the CCPA and to provide documentation supporting its analysis. While the definition of "service provider" is somewhat circular, questions to consider include whether the entity is collecting or "processing" personal information on behalf of covered businesses for a specified "business purpose," and whether the entity is restricted by contract from retaining, using, or disclose the personal information for any other purpose. Failing to adequately explain how the organization reached the conclusion that it qualified as a service provider could result in the OAG taking further action.

- **Ensure Proper Segmentation of Data**

  An organization contending it is a service provider must also be able properly segment the data it processes on behalf of covered businesses and implement the needed controls to avoid inadvertent violations of vendor contracts. This is especially critical for service providers who may be processing personal information for different purposes depending on the customer. Indeed, simply stating that personal information will not be used for any purpose other than that specified in the applicable vendor contract is likely insufficient. In addition, it would not be surprising for the OAG to "look under the hood" in the course of an investigation into either the service provider or a business it services, to confirm that the restrictions imposed by the vendor contract (and required by the CCPA to qualify as a service provider) are actually being complied with.

- **Review Marketing Materials and Privacy Disclosures**

  Service providers should review existing marketing materials and privacy disclosures to ensure that their position as a service provider is not being undercut by communications otherwise made by the company. For example, statements suggesting that the organization complies with the CCPA as a covered "business" (e.g., offering California consumers methods to submit CCPA requests) may raise confusion as to what role the entity has assumed. Though not required by the CCPA, service providers may consider including statements in privacy notices clarifying their position as a service provider, which may demonstrate the company's limited role to consumers and OAG.

- **Responding to Consumer Requests**

  As a service provider, has your organization agreed to respond directly to consumer requests on behalf of the businesses you serve? If so, be careful. Your response to the consumer should continue to distinguish your organization as the service provider, as opposed to the covered business. Any confusion as to which role you have assumed may trigger follow up from OAG.

- **Wearing Multiple Hats**

  Proper data classification and mapping will be essential to determine an entity's role under the CCPA, especially where an organization may be acting as a service provider on the one hand and a covered business on the other. Organizations will want to ensure they are properly classifying and mapping information to track when data is limited in use as a service provider or subject to the obligations imposed on a covered business. Without proper classification and mapping, the organization may be forced to apply the most restrictive rules across all data collected to comply with the CCPA (*i.e.*, treat the personal information if the service provider were actually a covered business). This would likely create additional compliance burdens and could also result in tension between the service provider and the business it is processing information on behalf of. Similar to the above, wearing multiple hats may also warrant adding language to public statements clarifying the organization's position under the CCPA depending on the circumstance. For example, if an organization is acting as a covered "business" when collecting information directly from consumers but a "service provider" when collecting information from a third party, the company's public statements may want to make that apparent. This may be accomplished, for example, by indicating that the role the organization assumes depends on the context of collection or the organization's relationship with the consumer and then elaborating from there.

CCPA: The Enforcement Series

Enforcement of the California Consumer Privacy Act ("CCPA") began July 1, 2020. Our privacy team at Troutman Pepper includes several attorneys who worked in an attorneys general office. This privacy regulatory team has identified six areas of enforcement likely to catch the California Office of the Attorney General's (OAG) attention, which arguably holds sole regulatory enforcement authority under the Act. This six-part series will focus on those areas of the law. Building on the experience of advising clients on the CCPA since its passage, our privacy compliance team will then discuss discrete strategies to minimize enforcement risk and bolster compliance efforts.

Key Enforcement Issues to Note:

- *Prior to initiating an enforcement action for an alleged violation of the CCPA, the OAG must provide businesses with a notice of alleged noncompliance and a 30-day opportunity to cure ("Notice and Cure Letter").*
- *As of July 1, 2020, certain businesses have received Notice and Cure Letters. Given the 30-day window to cure, it is likely that nothing will be made public about these early enforcement targets until August 1st (i.e., once the cure period elapses), at the earliest.*
- *The OAG may be selecting early targets for enforcement actions in various ways including, for example, based on consumer complaints submitted directly to the OAG or those made public on social media platforms (e.g., Twitter), or simply by scanning business' websites for noncompliance.*
- *Because the proposed regulations implementing the CCPA have not been finalized, the OAG can only bring an action based on an alleged violation of the CCPA (i.e., the statute) or a data breach, which went into effect January 1, 2020. It would not be surprising to see, however, the OAG argue a violation of the CCPA and seek remedial measures based on its interpretation as stated in the draft regulations. For additional information on the status of the proposed regulations, click **here**.*
- *If a company receives a Notice and Cure Letter from the OAG, we advise seeking legal counsel on how to respond to the OAG's request in a manner that minimizes business disruption but demonstrates a willingness to comply. Early and frequent communication and transparency will be key.*

Contacts

Ashley Taylor, Jr.
Partner
804.697.1286
ashley.taylor@
troutman.com

Sharon Klein
Partner
949.567.3506
sharon.klein@
troutman.com

Wynter Deagle
Partner
858.509.6073
wynter.deagle@
troutman.com

Ron Raether
Partner
949.622.2722
ron.raether@
troutman.com

Sadia Mirza
Associate
949.622.2786
sadia.mirza@
troutman.com

Lauren Geiser
Associate
804.697.1379
lauren.geiser@
troutman.com

Anne-Marie Dao
Associate
858.509.6057
anne-marie.dao@
troutman.com