

# How to Avoid Common IP Mistakes Made by Early-Stage Companies—Part 4: CCPA and Its Interplay With GDPR

By **Mark P. Kessler** and **Diane Moss**

*This is the fourth in a regular series relating to common IP mistakes early-stage companies make when building a business.*

The California Consumer Privacy Act (CCPA) is slated to become effective on January 1, 2020. If you are reading this article, you have some inkling of its comprehensive nature and its status as an unprecedented state privacy law. Although unquestionably influenced by the EU's General Data Protection Regulation (Regulation (EU) 2016/679, or the GDPR), CCPA is a unique framework. Although both CCPA and GDPR aim to establish privacy rights and enhance the protection of individuals' personal data accessed by entities in the context of commercial interactions, CCPA is distinct from GDPR and, in some ways, goes further than GDPR does. CCPA, which applies to online and offline interactions, has adopted a broader definition of the term "personal information" (which includes business contact data and online identifiers such as IP addresses), a new defined term "sale," distinct requirements in the areas of consent and privacy notices, an array of consumer rights, and the provision of a private right of action—on an individual or class action basis—for claims relating to data breaches. At the forefront of distinguishing features, however, is CCPA's requirement that certain companies provide individuals with the ability to opt out of the sale of their personal information.

Companies that are GDPR compliant have taken a huge leap toward compliance with CCPA; however, GDPR compliance does not equal CCPA compliance. Given the different emphases, and the broader reach of CCPA, companies will have to make adjustments

beyond existing GDPR compliance protocols. For companies that have not begun a GDPR compliance effort, the lift to become CCPA compliant is that much heavier. Below are some high-level areas to pay attention to as you navigate GDPR and CCPA compliance.

- 1. Does CCPA apply to my startup?** CCPA protects the personal information of California consumers (including all natural persons and business contacts located in California), and applies to businesses that control the processing of consumer personal information, service providers (indirectly as a processor through their relationship with the business they provide services to), and the catch-all category "third parties," which includes vendors other than service providers that a business is sharing data with. Any for-profit organization doing business in California that meets one of the following criteria is considered a business: (1) has an annual gross revenue of \$25 million or more; (2) buys, sells, receives, or shares for commercial purposes the personal information of 50,000 or more consumers on an annual basis, with "sale" being defined broadly 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"; or (3) derives 50 percent or more of its revenue from personal information sales. If you are a legal entity and have been engaged to process information

on behalf of a business, and the business will disclose a consumer's personal information to you for a business purpose pursuant to a written contract, you are a "service provider." Casting the net of applicability wider, CCPA subjects third parties to its authority, capturing any individual, legal entity, group, or organization that is not a business or service provider, or another recipient of personal information that has similar contractual restrictions with businesses as a service provider. With respect to third parties, it is important for businesses to identify what vendors they share information with and determine the type of decision-making control such vendors have over the information once it's been shared. This determination can trigger additional obligations for a business under CCPA (see question 5, below).

**2. What are the requirements for a company to comply with CCPA?** Privacy policies must disclose certain information, and service provider agreements must have specific language that prohibits service providers 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." Companies must also make sure service providers are able to respond to consumer requests for access to and deletion of their personal information. Companies are also obligated to provide two channels for consumers to request details regarding their personal information, such as a toll-free phone number and through their website. While GDPR obliges organizations to keep privacy notices current with respect to data collection, use, sharing, and processing practices, it does not impose time frames for review or updates. In contrast, CCPA imposes a specific requirement that privacy policies be updated annually. Similar to GDPR, but with less-stringent requirements, CCPA requires service providers and businesses to enter into a written agreement with affirmations on the use of the information that is disclosed for business purposes.

**3. How are the consent requirements under CCPA different from those under GDPR?** GDPR and CCPA stress the importance of transparency regarding the purposes of collection and require "just in time" notifications to consumers. CCPA offers consumers the right to opt out of the

"sale" of their personal information. By contrast, GDPR offers six lawful bases for processing personal information, including consent, and consent may be revoked at any time. GDPR's opt-in and opt-out processes are generally regarded as more rigorous than the opt-out framework adopted by CCPA.

**4. How does the CCPA grant consumers the right to access and control the use of their personal information by businesses?** CCPA has imposed obligations on companies to implement practices that enable the realization of new consumer rights. Under both GDPR and CCPA, individuals have the right to receive a copy of their personal information, which places responsibility on organizations to have processes in place that enable data to be provided to a requesting individual in a readily usable format, and to transfer the data directly to another organization. Given the breadth of "personal information" under CCPA, compliance requires that an inventory be conducted by every entity subject to the statute, and that appropriate technical tools be in place. Data deletion is another example. Subject to some exceptions, both frameworks require organizations to delete personal information from internal systems/ records upon consumer request and instruct service providers to do the same. CCPA includes a broader list of exceptions.

**5. Does CCPA require an organization to post a "Do Not Sell My Personal Information" link on its website's homepage and in its privacy policies?** Yes, if sharing of personal information by the business is determined to be a sale for "monetary or other valuable consideration." As referenced above, the term "sale" includes sharing, transmittal, and a host of other activities, so this inquiry is crucial. The disclosure or transfer of consumer personal information from a business to any third party may be deemed a sale unless the third party is solely using the information to fulfill a specific purpose on behalf of the business, a CCPA-compliant written contract is in place, and the business has provided the consumer with notice of the sharing and use. If a "Do Not Sell" link is required, then the business must post that link on its webpage and in its privacy policy, and the link must provide the capability to stop the sale of the personal information.

Undertaking a “data inventory” or “data mapping” process is essential to have a firm grasp of what personal information is collected (understanding the scope of the term “personal information”), the business purposes and any disclosures (understanding the scope of the term “sale”), and complying with CCPA. Retention practices should also be reviewed to limit the potential for stand-alone information not falling into the definition of personal information to be linked, integrated, or inadvertently morphed into “personal information” subject to protection under CCPA. The California attorney general recently released proposed regulations for CCPA, with a public comment period open until December 6. While the draft regulations provided some clarity on CCPA, they also imposed new and unexpected requirements. For more information on how the regulations may impact your startup, please see our Client Alert, “California Attorney General Releases Draft Regulations Under the California Consumer Privacy Act: New Concepts, New Questions, and Few Clarifications.”

CCPA grants consumers the right to pursue a civil suit and statutory damages (\$100-\$750 per incident or actual damages, whichever is greater) for a data

breach involving their personal information if a business fails to fulfill its obligations with respect to security. This private right of action and the imposition of statutory damages removes the burden from impacted consumers to prove or quantify the damage suffered as a result of a data breach and increases the possibility of more lawsuits to redress violations. Coupled with a consumer’s direct right to bring an action for a data breach are the broad enforcement powers granted to the Attorney General of California, who may bring a civil action in the name of the people for CCPA violations and seek injunctive relief. In these actions, civil penalties are capped at \$2,500 for each violation and \$7,500 for each intentional violation of CCPA.

Hence, it is important to understand how your business interacts with the personal information of California consumers, that a business does not have to be located in California to be subject to the state’s provisions, and that California hosts the largest population in the United States. It is quite possible California consumers are interacting with you.

## Contacts

### **MARK P. KESSLEN**

Partner

**T: 646.414.6793 (NY) / 973.597.2330 (NJ)**

[mkessler@lowenstein.com](mailto:mkessler@lowenstein.com)

### **DIANE MOSS**

Counsel

**T: 973.597.2448 (NJ) / 212.262.6700 (NY)**

[dmoss@lowenstein.com](mailto:dmoss@lowenstein.com)

---

NEW YORK

PALO ALTO

NEW JERSEY

UTAH

WASHINGTON, D.C.