California Consumer Privacy Act Overview and Checklist

Background

A first of its kind in the U.S., the California Consumer Privacy Act of 2018 (CCPA) is shaping up to be one of the most ambitious privacy legislations in the world; and with 17 additional states so far following its lead, data privacy protection is finally having its day in the United States. Effective January 1, 2020, the CCPA will become enforceable as early as next spring. More specifically, the Act will be enforced on the _earlier of_ either July 1, 2020 or 6 months from the date of issuance of the final regulations, following the California Attorney General's enforcement guidelines (expected mid-September).

Although the CCPA comes on the heels of the EU's General Data Protection Regulation (GDPR) and shares some similarities with it, the CCPA is its own unique legislation in many ways, including its stated purpose. Enacted as a clear response to the sizable data breaches impacting U.S. citizens over the past several years (Facebook, Sony, Equifax, to name a few), the CCPA is designed to give California consumers ownership and control of their personal information, and the right to hold businesses accountable for such information which they collect and handle as part of their business operations.

Key Provisions

The CCPA gives California consumers enhanced rights with respect to their personal information, including the right to know what personal information is being collected, how it is being used, whether their information has been disclosed or sold to third parties, and to whom, and the right to oppose the sale of their information to third parties. Because the CCPA is a markedly different piece of legislation than the GDPR, affected companies should not assume their GDPR compliance efforts will satisfy the requirements of the CCPA.

Below is a list of key CCPA provisions that will impact corporate compliance efforts:

• **Scope of applicability** – The CCPA only applies to for-profit companies which collect and handle the personal information of Californians, regardless of a physical location in the state, and which meet one of the following criteria: (a) annual gross revenue in excess of $25M, (b) receive or share personal information of more than 50,000 California consumers annually, or (c) derive at least 50% of annual revenue from the sale of personal information of CA consumers.

• **Consumers** – The CCPA defines a "consumer" as a natural person who is a CA resident. Under CA law, residents include (a) individuals in the state for other than temporary or transitory purposes, and (b) individuals domiciled in the state who are outside the state for temporary or transitory purposes. Because the definition of consumer is not limited to buyers of goods and services, it could arguably include others, such as a company's employees residing in CA. The CCPA's protections also apply regardless of how a business identifies an individual consumer, including by any unique identifier, household, or device.

• **Personal Information** – The statutory definition of Personal Information under the CCPA is particularly broad and includes, without limitation, an email address, an IP address, a person's education, employment or employment history, commercial information (i.e. records of personal property and purchasing habits), biometric information (i.e. genetic, physiological, behavioral, and biologic characteristics, or activity patterns), internet or other similar network activity, geolocation data, as well as inferences drawn from other personal information to create consumer profiles.

• **Right to opt out** – Perhaps the most important right granted to consumers under the CCPA is the right to opt-out of sales of their personal information to third parties. It is important to note that the CCPA's definition of "sale" is particularly broad and includes any communication or transfer of a consumer's personal information to another business or third party for monetary "or other valuable consideration," thereby encompassing situations in which a business receives any type of benefit in return for providing access to the personal information. Examples of valuable consideration include mutual access to each business's marketing list, access to information or insights about consumers, or the ability to target advertising to specific consumers.

The Act requires businesses to provide notice about the consumer's opt-out right by adding a conspicuous, separate and dedicated "Do Not Sell My Personal Information" link on their home page where consumers can exercise this right. For consumers between the ages of 13-16, opting out is not enough; the consumer must opt-in to having their personal information sold. For consumers under the age of 13, parental consent is required.

• **Right to know/access** – Consumers also have the right to know and to request access to their personal information collected by a business, including information about what categories of personal information have been collected, disclosed or sold, categories of sources from which the information was collected, categories of third parties receiving the personal information; and the purpose for collecting or selling such information. Additionally, consumers have the right to know specific pieces of personal information collected by a business (not just the categories).

• **Right to portability and deletion** – Under the CCPA, consumers requesting access have the right to also know the specific pieces of personal information the business has collected (not just by categories) and to receive their personal information in a "readily usable format" that is also portable, free of charge and delivered within 45 days of their request. Additionally, they have the right to request the deletion of their personal information collected, subject to certain limited exceptions. Businesses are required to offer at least 2 separate methods by which consumers can make portability and deletion requests.

• **Right to equal services and price** – The CCPA prohibits businesses from discriminating against CA consumers in retaliation for exercising their rights under the law. However, they are

permitted to offer different prices or levels of service, if such differences are reasonably related to the value provided to the consumer by the consumer's personal information.

• **Private right of action** – The CCPA mandates that businesses protect the personal information of California consumers, and gives consumers the right to sue a company directly if their personal information was not properly protected such as by encryption or redaction.

• **Disclosure of personal information sold** – Under the CCPA, businesses that sell or disclose personal information for business purposes will be required to disclose certain information to consumers upon receipt of a verifiable consumer request. In connection with this requirement, they must also maintain separate listings for data collected, sold or shared for business purposes and for commercial purposes.

• **Privacy policy disclosures** – In addition to the disclosure requirement provided for as part of the right to know and access, businesses complying with the CCPA must make certain affirmative disclosures about their privacy practices in both their external privacy policy and in their privacy notice to their California employees, including an enumeration of the categories and specific pieces of personal information being collected, the sources from which such information is collected, the purpose of the information, and the categories of third parties with whom the information will be shared.

CCPA Readiness Checklist

Companies doing business with CA consumers should prepare to comply with the CCPA as early as possible to avoid the risk of severe financial penalties. To start, businesses should conduct a comprehensive review of their current data privacy practices, policies and procedures. The below checklist is intended to guide your efforts:

___ **Confirm applicability of CCPA –** Start by determining if your company meets the applicability criteria.

___ **Analyze the collection, storage and processing of data about California residents that falls under the scope of "Personal Information" in the CCPA –** Start by creating a detailed and centralized mapping of your collecting and handling activities.

___ **Update customer and employee/applicant-facing privacy policies and notices** – Review your privacy policies to ensure they comply with the CCPA disclosure requirements.

___ **Update your website to include an opt-out link** – If your company sells the personal information of CA consumers, you must create a separate web page titled "Do Not Sell My Personal Information" which allows consumers to opt-out without requiring account creation.

___ **Update vendor agreements and template contracts --** Review and update all current vendor agreements and contract templates to comply with the CCPA rules.

___ **Update customer contracts** – Review terms of use and other customer contracts and templates to ensure there are no provisions which waive customer rights to request data.

___ **Update service provider agreements** – Review current service provider agreements to ensure that the CCPA-mandated provisions are included.

___ **Create/update procedures for receiving and processing user access requests and complaints** – Organizations must implement internal procedures to respond to a consumer requests, as permitted under the CCPA, within 45 days of their receipt.

___ **Evaluate existing information security policies and procedures in light of the CCPA private right of action.**

___ **Assess whether any programs, offers or incentives (e.g., loyalty programs) may be considered discriminatory under the CCPA**.

___ **Assess whether financial incentives are offered to California residents for use of their personal information.**

___ **Create/update record keeping procedures and policies** – The CCPA requires companies to maintain separate listings of data collected, sold or shared for business purposes and commercial purposes. A system for tracking opt-out requests should also be implemented.

___ **Conduct employee training on CCPA-mandated requirements, processes and procedures and update employee guidance and policies –** Educate and train employees on new CCPA privacy protection requirements and processes, including, most importantly, how to handle opt-out requests.

___ **Periodic employee monitoring and security checks for compliance** – Conduct periodic reviews of employee practices and security protections to confirm compliance with CCPA requirements.

Outside GC is well-positioned to assist in your compliance efforts. Our team includes U.S and EU-trained attorneys experienced with data privacy requirements and well-versed in the new obligations imposed by the CCPA, as well as the data privacy laws and regulations of the EU and Canada.

Stephan Grynwajc served as a senior in-house attorney for several blue-chip technology corporations (e.g., Intel and Symantec) in France, the U.K. and the U.S., and today, focuses his practice on advising U.S.-based clients on navigating the EU privacy landscape.

Mark Johnson has over 20 years of experience advising clients on data privacy regulations and public policy, and is a former member of the Data Privacy practice group at the international law firm, Squire Patton Boggs in Washington D.C.

Bill Porter is a member of our California-based team and brings over 20 years of experience representing technology companies at various stages of growth, handling a range of legal and business issues including privacy and data security matters.

Lakshmi Sarma Ramani served as the lead global attorney for privacy matters at The Nature Conservancy, where she also managed a wide range of legal and regulatory compliance matters, including cybersecurity, tax, finance, technology, marketing, membership and fundraising.

We would be happy to discuss your specific needs. Feel free to reach out directly to Stephan (Stephan@outsidegc.com), Mark (mjohnson@outsidegc.com) or Lakshmi (lsramani@outsidegc.com), or request more information by visiting our Contact Us page.