ALERT MEMORANDUM

California's Groundbreaking Privacy Law: The New Front Line in the U.S. Privacy Debate

July 13, 2018

On the heels of the European Union's implementation of the General Data Protection Regulation ("GDPR") and public outcry over the Cambridge Analytica scandal, on June 28, 2018, California enacted the most comprehensive data privacy law to date in the United States. The California Consumer Privacy Act of 2018 (the "CCPA") was hastily passed by the California legislature to secure the withdrawal of an even more far-reaching measure that had qualified for the November ballot. The sponsor of that initiative had agreed to withdraw the ballot measure if the legislature passed the bill prior to the withdrawal deadline, given the difficulty of making any revisions to a measure enacted by initiative rather than the legislature. Legislative amendments to the law are expected before it goes into effect on January 1, 2020, and the law requires the California Attorney General to develop certain implementing regulations.

The CCPA requires covered businesses to comply with requirements that give California consumers broad rights to know what personal information has been collected about them, the sources for the information, the purpose of collecting it, and whether it is sold or otherwise disclosed to third parties. It also gives consumers the right to access personal information about them held by covered businesses, to require deletion of the information and/or to prevent its sale to third parties. Other key provisions limit the ability of a covered business to discriminate against consumers who exercise their rights under the statute by charging them higher prices or delivering lower quality products or services.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

Michael Krimminger
+1 202 974 1720
mkrimminger@cgsh.com

Katherine Carroll
+1 202 974 1584
kcarroll@cgsh.com

Pam Marcogliese
+1 212 225 2556
pmarcogliese@cgsh.com

Jon Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Daniel Ilan
+1 212 225 2415
dilan@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

Alexis Collins
+1 202 974 1519
alcollins@cgsh.com

Gareth Kristensen
+1 212 225 2272
gkristensen@cgsh.com

Jane Rosen
+1 212 225 2026
jcrosen@cgsh.com

Martha Vega-Gonzalez
+1 212 225 2544
mvega-gonzalez@cgsh.com

Anne Hilby
+1 202 974 1635
ahilby@cgsh.com

Who must comply? As passed, the CCPA is likely to affect not only many California businesses, but a large number of businesses that merely have an online presence in California.

The CCPA applies to for-profit entities, located anywhere in the world, that do business in California, collect (or engage a third party to collect) the personal information of California residents and satisfy at least one of the following: (i) have over $25 million in annual gross revenue, (ii) buy, sell, or receive or share for commercial purposes, the personal information of 50,000 or more California residents, households or devices (households and devices are not limited to those in California or owned by California residents), or (iii) derive 50 percent or more of their revenue from the sale of personal information of California residents (any such entity a "covered business"). It also applies to any parent or subsidiary of a covered business that uses the same branding.

What personal information is covered? The CCPA's definition of personal information is significantly broader than is generally used in other U.S. laws. The CCPA definition covers "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with" a particular California resident *or household* (household is not limited to California). Examples include: IP addresses; purchasing or consuming histories or tendencies; browsing history; search history; information regarding a person's interaction with an Internet web site, application, or advertisement; "audio, electronic, visual, thermal, olfactory, or similar information"; and "inferences drawn" from any personal information to create a profile reflecting the resident's "preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."

What rights does the CCPA create for California consumers? The CCPA expands the rights of "consumers" (defined in the Act as natural persons who are California residents, which leaves some uncertainty about whether the Act could be interpreted to extend rights to employees vis-à-vis their employers, though this does not appear to be the intent) over their personal data in five key ways:

— *Right to Access and Portability*. Consumers have the right to request, up to two times every 12 months, disclosure by a covered business of the categories and specific pieces of personal information the covered business has collected about them, the categories of sources of such information, the covered business's purposes for collecting or selling personal information and the categories of third parties with whom the covered business shares such information. In addition, they have a right to know whether a covered business sells, or discloses for a business purpose, their personal information and, if so, the categories of personal information sold or so disclosed and the categories of third parties to whom the personal information was sold or so disclosed, in each case during the 12 months preceding the request. Upon a verifiable consumer request, covered businesses must disclose and deliver the requested information free of charge within 45 days (or 90 days if the business gives the consumer notice it needs an extension). Such information shall be delivered by mail or electronically, and if electronically, "in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information … to another entity without hindrance." This goes beyond California's existing "Shine the Light" law, which requires businesses to make certain disclosures to their California customers with respect to the sharing of their personal information with third parties for marketing purposes unless such customers are given the opportunity to opt out of such sharing.

— *Right to Require Deletion.* Consumers have the right to require the covered business to delete their personal data. Upon a verifiable consumer request, a covered business must delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their

records. The CCPA provides exceptions to this requirement where it is necessary for the business or service provider to maintain the consumer's personal information, including for the purposes of completing a transaction, exercising free speech, complying with a legal obligation, enabling "solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business" or otherwise using the information "internally, in a lawful manner compatible with the context in which the consumer provided the information."

— *Right to Prohibit Sale*. Consumers 16 years or older have the right to request that the covered business refrain from selling their personal data. Once a covered business has received such an "opt-out" request, it may not seek that consumer's authorization to sell his or her personal information for at least 12 months. For consumers under the age of 16, a covered business may not sell their data without their (or in the case of persons under age 13, their parent's) express consent.

— *Right to Equal Treatment*. Covered businesses are prohibited from discriminating against consumers who exercise any of their rights under the CCPA, including by charging a different price or providing a different quality of goods or services, except if the difference is reasonably related to value provided to the consumer by his or her data. Covered businesses may, however, offer financial incentives for collection, sale or deletion of personal information, provided the incentives are not "unjust, unreasonable, coercive or usurious."

What affirmative obligations does the CCPA impose on businesses? The CCPA imposes several obligations on covered businesses, including some that may require such entities to reexamine and revise internal processes for identifying and processing data that falls under the CCPA's expansive definition of personal information. Under the CCPA, covered businesses must:

— *Comply With Verified Requests From California Consumers.* Upon receiving a verifiable request from a consumer for data access or deletion, a covered business must comply with the request, as described above. A covered business must, therefore, implement processes to enable it to identify the personal information it has collected about any consumer and provide it to the consumer in the required format or delete it, as applicable. Similarly, covered businesses will need to implement a verification process in order to verify the requests are from or on behalf of the consumer purportedly making the request.

— *Provide Request Mechanisms*. Covered businesses must make available two or more designated methods that consumers may use to submit requests, including a toll-free number and website address, if the business maintains a website.

— *Post "Do Not Sell" Links*. A covered business must post a clear and conspicuous link titled "Do Not Sell My Personal Information" on its homepage that will enable consumers (or their authorized agents) to opt out of the sale of such consumers' personal information. Covered businesses will need to implement mechanisms to track opt outs and ensure they do not seek authorization from consumers who have opted out for at least 12 months after such opt out.

— *Include CCPA Disclosures in Their Privacy Policies*. Covered businesses must update their privacy policies (or their websites if they do not maintain a privacy policy) at least once every 12 months to (a) describe the rights of consumers under the CPPA and (b) list categories of information collected, sold or disclosed for a business purpose during the preceding 12 months.

What are the penalties for non-compliance? The California Attorney General is responsible for enforcement of the CCPA. Covered businesses that fail to cure an alleged violation within 30 days' notice of alleged noncompliance could face a penalty of up to $7,500 per violation if the violation is deemed intentional.

Additionally, the CCPA allows private litigants to sue covered businesses in the aftermath of data breaches, providing for statutory damages ranging between $100

and $750 per person per incident (or actual damages, if greater) where the consumer's personal information (defined more narrowly than in the rest of the statute) is stolen or disclosed through unauthorized means as a result of a covered business's failure to implement and maintain reasonable security procedures. This is, however, subject to a requirement to notify the California Attorney General and allow the California Attorney General to instead prosecute the covered business itself if it so chooses.

How does the CCPA compare to the GDPR? Some public commentary has described the CCPA as "California's GDPR" or "GDPR-lite." While the CCPA appears to draw inspiration from the GDPR – under both laws, individuals have rights of transparency, access and data portability and rights to instruct deletion with respect to their personal data – there are distinctions in approach on some key issues.

Generally speaking, the CCPA is less onerous than the GDPR. For example:

— *General Ability to Lawfully Process Personal Data*. The GDPR includes certain conditions that must be met for a business's collection, use, storage and other processing of personal data to be lawful, including that the processing must be based on one of several prescribed lawful grounds. The default position is therefore that the processing of personal data is unlawful unless it is done on the basis of one of these prescribed grounds. The conditions that must be met in order to rely on some of these grounds can be onerous – for example, if a business processes personal data on the basis of a person's consent, the GDPR requires such consent to have been freely given, specific, informed and unambiguous. The CCPA does not include such broad restrictions on companies' abilities to process personal data. Instead, it focuses on providing transparency (for instance, by giving notice to consumers at or before the point of collection as to the categories of personal information to be collected and the purposes for which it will be used) and providing the consumer with certain rights to restrict sale and require deletion of their data.

— *Opt Out vs. Opt In*. The CCPA requires businesses to allow consumers an opportunity to opt out of the sale of their personal information. Under the GDPR, businesses are unlikely to be permitted to sell a person's data unless the person freely gives specific, informed and unambiguous consent to the sale.

— *Vendor Contracts*. While the CCPA contains strong incentives for businesses to include certain requirements in contracts with service providers, such as prohibiting service providers from selling personal information shared with them or using it for purposes other than performing services specified in the contract, the CCPA is less prescriptive than the GDPR, which requires specific additional terms to be included in contracts with third-party vendors who are appointed to store and process personal data on behalf of another business.

— *Cross-Border Transfers*. Unlike the GDPR, which restricts transfers of personal data outside of the European Economic Area unless certain requirements or exemptions are met, the CCPA does not restrict the transfer of personal information outside of California's jurisdiction.

At the same time, even a covered business that is already in compliance with the GDPR may have to consider the following ***additional compliance obligations under the CCPA***:

— *Anti-discrimination*. As discussed above, the CCPA bans covered businesses from discriminating against California residents that exercise their rights under the CCPA, including by charging a different price or providing a different quality of goods or services (though businesses may offer certain financial incentives for the collection or sale of personal information). In contrast, price discrimination might be permissible under the GDPR, provided the individual freely gives specific, informed and unambiguous consent (though consent is unlikely to be regarded as freely given if the provision of a service is made conditional on the provision of consent to process

personal data that is not necessary for performance of the contract).

— *Specific Request Mechanisms*. The CCPA includes certain specific compliance requirements for providing consumers with mechanisms to make access and deletion requests. Such mechanisms are not found in the GDPR.

* * *

Ultimately, it is likely that the CCPA will be subject to amendment and clarification before it enters into force on January 1, 2020. Various provisions are vague, contain clear errors, such as references to non-existent provisions, or appear internally inconsistent. Nevertheless, assuming the CCPA's basic framework remains in place, covered businesses, even those that are already complying with the GDPR, will likely need to assess the way they currently collect, sell, and store personal information and build mechanisms to comply with requests of California residents.

It also remains to be seen whether other states (or Congress) will follow California's lead and adopt similar laws. In 2002, California enacted the nation's first data security breach notification law, but it was not until 2018 that every state in the country had such a law on the books. In the absence of a comprehensive federal regime, these laws have formed a patchwork of notification requirements for companies that have suffered hacks and other data breach incidents. While most states have enacted data breach notification statutes that follow a similar structure, each state's law includes nuances on significant issues such as what is considered a breach, who needs to be notified when a breach occurs, and when and how such notification must occur. If a similar patchwork evolves with respect to broader privacy rights like those covered by the CCPA, companies could be forced to navigate different (and potentially conflicting) state privacy requirements in the ordinary course of conduct of their business. If the momentum for such expanded privacy rights builds through new state laws, and compliance with early state requirements and the GDPR demonstrate the business feasibility of addressing them, pressure might grow on Congress to adopt a comprehensive national scheme.

…

CLEARY GOTTLIEB