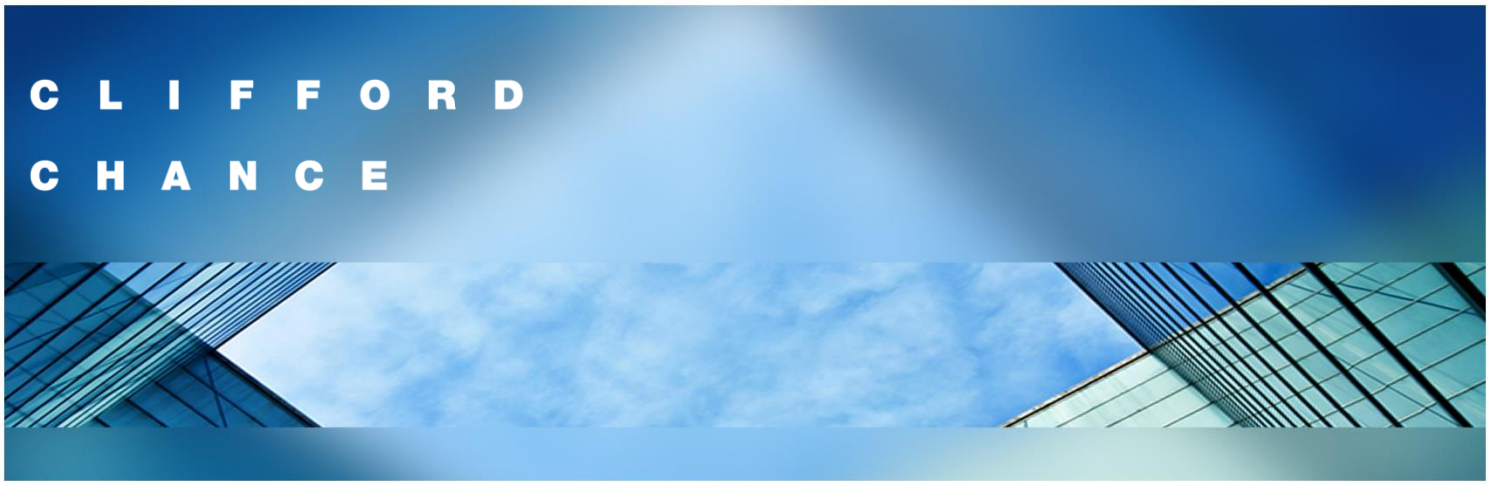

CALIFORNIA CONSUMER PRIVACY ACT TAKES SHAPE: AMENDMENTS AND DRAFT REGULATIONS PROVIDE SOME CLARITY BUT QUESTIONS REMAIN

On Thursday, October 11, 2019, the California Attorney General (AG) issued long-awaited draft regulations for the California Consumer Privacy Act (CCPA), the landmark state law that will dramatically increase the standard of data privacy and cybersecurity protections required of companies that do business in California.[1] In addition to providing guidance on many elements of the CCPA, the regulations also impose several new, unexpected requirements on businesses. And despite the additional guidance, questions remain, including what impact several amendments signed by Governor Newsom just a day after the draft regulations were issued will have on businesses that do business in California.

The Draft Regulations

The draft regulations issued by the California AG elaborate on a range of CCPA provisions, including:

- how to make notices "easily understood by the average consumer" or accessible to consumers with disabilities (as required by the law);
- the required content that must be in a business's privacy policy;
- how companies should verify consumer requests based on the sensitivity risk associated with the request; and
- what entities qualify as "service providers" under the law and the scope of their obligations.

The regulations also clarify how certain provisions apply in specific situations, such as whether businesses that do not collect personal information directly from

[1] For more information on the law itself, see our previous briefing.

consumers need to provide initial notices (they do not) and whether businesses that engage with consumers offline must still provide notices (they do).

Perhaps most important are the provisions in the regulation that could be considered additional requirements or extensions of the law, including:

- requiring a business seeking to use personal information for a purpose other than those disclosed at collection to obtain explicit consent from a consumer (in contrast to just providing additional notice, as required by the statute);
- requiring a process to allow an authorized third-party to make CCPA rights requests on a consumer's behalf;
- imposing a 10-day time limit to acknowledge receipt of a consumer request in addition to—and within—the 45-day deadline set forth by the CCPA to verify and comply with a request;
- requiring businesses to take certain actions even for unverified consumer requests, such as providing directions on how to remedy deficient requests or treating an unverified deletion request as a request to opt out of a sale;
- requiring businesses to acknowledge privacy controls, such as a browser plugin, as a valid opt-out request;
- requiring businesses to respond to opt-out requests within 15 days and notify all third parties to whom it has sold personal information of the consumer within 90 days prior to such a request;
- exempting particularly sensitive information from disclosures in response to a verified consumer request, including Social Security number or other government-issued identification number, financial account number, health insurance or medical identification number, an account password, or security questions and answers;
- requiring businesses to maintain records of consumer requests and how the business responded to such requests for at least 24 months;
- requiring businesses that collect or share personal information of more than four million California consumers to report on CCPA-related metrics such as the number of consumer requests received in the previous calendar year and the median days taken to respond to such requests;
- raising the bar on what is required to obtain consent from consumers under age 16; and
- requiring businesses to estimate—and explain—the value of a consumer's data where a business provides a financial incentive or offers different prices or services based on a consumer's privacy choices.

Notably, the regulations do not answer certain key questions about the CCPA, including what is considered "doing business" in California. Significantly, the regulations also fail to provide additional guidance on whether certain nuanced instances of data disclosures or transfers could be considered a "sale" of personal information under the law.

Amendments and Related Laws

The draft regulations do not address the amendments passed by the California legislature last month and signed into law on October 11 (the day after the rules were issued). Most of the changes to the law made by the amendments were relatively minor, including modifications such as eliminating the requirement for businesses that solely operate online to have a toll-free number to field consumer rights requests. However, two amendments created key exemptions from the law for employee data and personal information collected as a result of business-to-business transactions (such as contact information of a sales representative for a service provider). The amendments exclude this data from certain rights provided by the law such as the rights of access and deletion. Both amendments have sunset provisions, however, indicating that they are just stopgaps until the legislature is able to create a more comprehensive and long-term plan for employee and business-to-business personal information.

In addition to the amendments directly addressing the CCPA, the legislature passed two additional data privacy-related laws in September. The first law establishes a statewide data broker registry that requires any company that sells data to register its activities and pay an annual fee. The law's definition of "selling" personal information incorporates the CCPA's expansive definition, which includes any transfer from one entity to another for monetary or other valuable consideration. The second law expanded the information covered by California's existing data breach notification law to include tax ID numbers, passport numbers, military ID numbers or other unique ID numbers issued on a government document as well as some biometric data. Companies undergoing compliance efforts will need to take into consideration additional obligations imposed by both new laws.

What's Next

While the amendments and regulations provide additional clarity on how data privacy requirements will be enforced in California, many questions linger and more remains to be done before enforcement begins in the middle of 2020. Privacy advocates and members of industry are closely scrutinizing the regulations and preparing comments, which the California AG has stated it will accept until December 6, 2019, both online as well as during a series of public hearings scheduled throughout the state in the beginning of December. Meanwhile, certain legislators indicated that additional amendments and a longer-term plan for employee and business-to-business personal information will be considered when the legislature reconvenes for the 2020 session. At the same time, some privacy advocates have taken more radical measures, including announcing plans for a new ballot initiative for 2020—the CCPA 2.0—that would create a new data privacy enforcement agency and create even more stringent requirements. And in the background, efforts to adopt a federal data privacy law continue.

All of this places companies in a difficult position as they grapple with compliance in a rapidly-changing data privacy landscape. Despite this uncertainty, however, businesses cannot afford to wait to begin their compliance efforts. While July 2020 may seem distant now, those who were responsible for ensuring compliance with the General Data Protection Regulation (GDPR) know how much of a task it

is to update their policies and procedures for a comprehensive new law such as the CCPA. Companies should begin preparing now to avoid the compliance crunch many faced in the lead-up to GDPR enforcement.

CLIFFORD
CHANCE

CONTACTS

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Steven Gatti
Partner

T +1 202 912 5095
E steven.gatti
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

Kaitlyn Ferguson
Associate

T +1 202 912 5190
E kaitlyn.ferguson
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 2001 K Street NW, Washington, DC 20006-1001, USA

Clifford Chance US LLP