Paradigm®

INTERNATIONAL SOCIETY OF PRIMERUS LAW FIRMS

SPRING 2019

President's Podium: Primerus Community

Relationships Form the Bedrock of the Primerus Community

Current Legal Topics:

Asia Pacific
Europe, Middle East & Africa
Latin America & Caribbean
North America

Primerus Law Firm Directory
Page 51

California's Consumer Privacy Act: Implications for Counsel and Clients

On June 28, 2018, California Governor Brown signed the California Consumer Privacy Act (CCPA), which will become effective on January 1, 2020. The CCPA (Civil Code § 1798.100 *et seq*.), is the most significant state privacy legislation passed in the United States for many years. The CCPA has been compared to the most important privacy legislation of recent years – the European Union's General Data Protection Regulation (GDPR), which came into effect on May 25, 2018.[1]

Having only recently undertaken substantial efforts to comply with the GDPR, including revising privacy and other policies, many companies in the United States may well be wary of having to undertake new work to comply with the privacy legislation passed by a single state. Whether such efforts are required will depend on the extent of California consumer data collected and shared by a business and whether the CCPA will be modified or preempted by federal legislation before it comes into effect.

Timothy Toohey

Timothy Toohey leads Greenberg Glusker's cyber security practice, working to assure that his clients' proprietary, personal, customer and employee information, and other sensitive data is fully protected and serves its intended purposes. He is a United States and European Union Certified Information Privacy Professional and a Certified Information Privacy Manager.

Greenberg Glusker
1900 Avenue of the Stars
21st Floor
Los Angeles, California 90067

310.553.3610 Phone

ttoohey@greenbergglusker.com
greenbergglusker.com

What is the CCPA?

The CCPA forestalled a substantially stricter privacy measure sponsored by Californians for Consumer Privacy, headed by San Francisco real estate developer Alastair Mactaggart, that had qualified as an initiative for the Fall 2018 ballot. Because the California legislature passed the CCPA in relatively short time, the technology industry, privacy professionals and advocacy organizations continue to lobby the California legislature to modify the CCPA. However, barring unforeseen changes and timely promulgation of regulations by the California Attorney General, enforcement of the CCPA will commence on July 1, 2020.

Four aspects of the law are particularly salient for businesses considering whether their operations fall under the CCPA:

- The CCPA imposes substantive new obligations on companies "doing business in California"[2] to protect the "personal information" of California "consumers." "Personal information" is broadly defined as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." A "consumer" is a "natural person who is a California resident," including employees, parents and children.
- The CCPA is applicable to a for-profit business (wherever located) if it (1) has annual gross revenues in excess of $25 million; (2) "annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices;" or (3) derives 50 percent or more of its annual revenues from selling consumers' personal information.[3]
- The CCPA gives California consumers substantive new rights, including: (1) the right to obtain information regarding the categories and specific pieces of personal information collected by the business about that person; (2) the right to make requests regarding the information held by the business about them; (3) the right to obtain (free of charge) copies of the personal information held by the business; (4) the right to request deletion of certain personal information; and (5) the right to direct a business that "sells" personal information to third parties not to sell such information ("opt out right").[4] For the purpose of the statute, "sell" is broadly defined as including "releasing, disclosing, disseminating, making available, transferring, or otherwise communicating … a consumer's personal information."[5]
- The CCPA gives the California Attorney General enforcement authority and the power to levy sanctions of $7,500 per intentional and $2,500 for unintentional

violations.[6] The statute also creates a private right of action with statutory damages for security breaches, which are defined as "unauthorized access and exfiltration, theft or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices."[7]

Is the CCPA another GDPR?

Although the CCPA's definition of "personal information" is strikingly similar to the GDPR's definition of "personal data" and the CCPA provides increased consumer rights, similar to those of the GDPR, the CCPA is far from being a GDPR clone. Unlike the GDPR, the CCPA is not a comprehensive privacy regulation applying to all business sectors. The CCPA specifically exempts health and some financial information from its scope.

The CCPA, unlike the GDPR, also does not require a specific legal basis for collection and processing of data. Nor does the CCPA require companies to hire data protection officers or enter into data processing agreements. The CCPA also does not prohibit trans-border data transfers, nor will the California Attorney General be able to levy fines and penalties on the high level of EU data protection authorities.

Will there be federal privacy regulation?

Notwithstanding the CCPA's relatively limited scope, its passage has led to a renewed push for federal legislation that could preempt state laws like the CCPA. By early 2019, a half-dozen proposals have emerged with no clear frontrunner.

Citing the data collection and sharing practices of companies like Facebook and Google, as well as the data breaches involving Marriott and Equifax, several Democrats have called for a comprehensive and strict privacy law to hold companies responsible for their data practices. For example, Democrats have introduced a bill to enact a fiduciary-like standard of care on organizations collecting personal data and, separately, a Consumer Data Protection Act with "radical transparency for consumers" that would allow the FTC to fine companies and send corporate executives to jail.

In contrast, Republicans and large U.S. companies propose passage of a federal law to preempt what Intel calls "[a] non-harmonized patchwork of state legislation."[8] Similarly, Senator Marco Rubio's proposed pre-emptive federal act would promote transparency without harming "innovative capabilities."

Should businesses ignore the CCPA and wait for federal privacy legislation?

The future of federal legislation is uncertain, given the partisan divide in Washington. But pending passage before January 1, 2020, of a comprehensive law preempting state laws (which seems unlikely), companies doing business in California should consider whether they meet the criteria of the CCPA by having gross receipts of $25 million or annually collecting data of 50,000 or more Californians, i.e., 137 records a day.

If a business is subject to the CCPA, it will likely have to modify its privacy policy and establish a mechanism for complying with consumers' requests for information and limited rights of data transfer and erasure. Under the CCPA's broad definition of "sell," a business sharing information with third parties must not only describe its practices and give notice to California consumers of their rights, but also post a clear and conspicuous link on its website titled "Do Not Sell My Personal Information" to allow consumers to exercise their opt-out rights.

Businesses should also be aware that the California Attorney General's office is likely to take an active enforcement role under the CCPA through fines and penalties. Companies should also be alert that, for the first time, plaintiffs may bring lawsuits with statutory damages for certain data breaches.

Although it is unclear whether the CCPA is the harbinger of a new era in federal privacy legislation, the law is likely to have an outsized impact on other states, emanating as it does from the heart of the technology industry. If earlier legislation like California's pioneer data breach notification law is any indicator, other states may also be inspired to follow the example of the CCPA and strengthen their own privacy laws. In any event, companies should monitor the situation carefully and begin compliance efforts well ahead of the effective date of the CCPA. P

1 fpf.org/2018/11/28/fpf-and-dataguidance-comparison-guide-gdpr-vs-ccpa/

2 "Doing business in California" is defined by the California Franchise Tax Board as "actively engaging in any transaction for the purpose of financial or pecuniary gain or profit." *See* ftb.ca.gov/businesses/Doing-Business-in-California.shtml

3 Cal. Civil Code § 1798.140.

4 Cal. Civil Code §§ 1798.100-120

5 Cal. Civil Code § 1798.140

6 Cal. Civil Code § 1798.155

7 Cal. Civil Code § 1798.150

8 securityweek.com/intel-asks-comments-draft-federal-privacy-law