CYBERSECURITY, PRIVACY AND DATA PROTECTION ALERT

Getting Started With The California Consumer Privacy Act

By: Daniel S. Marvin & Karl Rumph*

As you may be aware, the California Consumer Privacy Act of 2018 ("CCPA" or "the Act") came into effect on January 1, 2020, and provides California residents with as much control as feasibly possible over the use of their personal information within the business world. In large part, the Act places obligations on qualifying businesses to notify California residents about how their personal information – defined broadly 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" – is being utilized, and to comply with requests made by the consumer with regard to their information. Now that the California Office of Attorney General ("OAG") has released its final set of CCPA proposed regulations, there has never been a better time for organizations to review their existing procedures, or to implement a CCPA compliant privacy program.

California has most certainly raised the stakes when it comes to data protection. Under the Act, the OAG can bring a lawsuit on behalf of California consumers against a non-complying business which may result in penalties of $2,500 for each violation, or $7,500 for every intentional violation, that is not cured within 30 days of notice. Moreover, if a consumer's information is accessed by an unauthorized actor as a result of a business's failure to reasonably secure the information, the Act provides individual consumers with their own private cause of action; damages can range anywhere between $100 and $750 for each consumer that is harmed in each incident.

Compliance with the CCPA can seem complicated, and, in many respects it is. Some companies must fully revamp, or even create, their internal processes for responding to verifiable consumer requests, and businesses must be aware of the pitfalls and consequences of falling out of compliance with the Act. While full disclosure and transparency can be a daunting task to undertake, this memorandum (the first in a series) aims to provide some clarity on how to get started with CCPA compliance.

MORRISON MAHONEY LLP

I. Is Your Business Subject to the CCPA?

The first question under the Act is to determine whether your business is active within the State of California to the extent that you are subject to the provisions of the CCPA. The Act revolves around the protection of "consumers' personal information," which includes any information that could reasonably be capable of identifying a California resident, either directly or indirectly. Under the CCPA, the term "business" refers to any legal entity that operates for profit, at the behest of shareholders or other owners, collects consumers' personal information, does business within the State of California, *and* satisfies one of the following:

(1) has an annual gross revenue in excess of twenty-five million dollars;
(2) buys, sells, receives, or shares the consumer information of at least 50,000 California residents (individually, by household, or device); *or*
(3) derives 50% of its annual revenue by selling consumers' personal information.

One thing to keep in mind is that because the California Legislature implemented a broad definition of "personal information," a business should consider any form of information which is remotely related to a consumer's identity as satisfying the definition. According to the Act, personal information can even include a consumer's "browser history," even if the consumer's name is nowhere to be found, so businesses should be mindful when any such information is collected. If the business collects or sells personal information, the next questions it must ask are (1) do they handle the personal information of over 50,000 California residents, and/or (2) does the sale of California consumers' personal information account for at least 50% of the business's annual revenue, either of which would bring such business within the purview of the Act.

In addition, when considering the question of if personal information is being sold, it is important to note that the "selling" of information can take the form of any exchange of valuable consideration, not strictly monetary. For example, a business may be considered selling information when they trade the personal information they've collected from consumers, in exchange for other goods and services to a third party.

II. What Does the CCPA Require?

The CCPA's rights and duties standards can be split into two general categories: (1) those that the consumer can inherently expect of the business; and (2) discretional rights held by the consumer personally. A qualifying business has a duty to include certain provisions in their disclosure statements and privacy policies regarding the nature and extent of their data collection, as well as an alert to consumers about those exercisable rights. Therefore, a business must have the appropriate procedures in place *prior* to the collection of data in order to be CCPA complaint.

A. The Business's Duties

All businesses that must comply with the CCPA need to have a Privacy Policy which conforms to a number of requirements. According to the OAG, the policy must notify consumers about the business's online and/or offline methods of collection, be easily identifiable and readable to the consumer, available in a format which can be printed by the consumer, and inform them of their right of request. If the business has a website, the policy must appear in the form of a link using the word "privacy," on the business's homepage, defined as the website's introductory page *and* any web page where personal information is

collected. Upon reading the Privacy Policy, and depending on the nature of the business, the consumer should be able to clearly understand what type of information is being collected, how it's being collected, and the purposes for its collection.

Moreover, a business must provide a "notice at collection," given at or before the point at which a business collects personal information from the consumer. Contained within this notice must be the categories of personal information the business plans to collect, along with their intended uses. Accordingly, any subsequent actions taken by the business must not be "materially different" from those disclosed in the notice of collection.

B. The Consumer's Rights

Contained within Article 3 of the California Consumer Privacy Act Regulations, promulgated by the OAG, are instructions as to how a business must handle a consumer's (1) request to know the information they've collected, (2) request to delete the information collected, or (3) decision to opt-out of the selling of their information to third parties. Each request comes with different requirements. For instance, there must be in place at least two designated methods available to a consumer who wishes to know the information the business has collected, one of which must include a toll-free telephone number. However, if the business operates exclusively over the internet, they only need to provide an email address where such requests can be submitted. One the other hand, requests to delete procedures must provide two or more methods of submission, regardless of the type of business, but without the need for a telephone number. In any event, any designated method proscribed must reflect to the nature of the business.

The varying levels of compliance obligations is also apparent when a consumer decides to opt-out of the sale of their personal information. While requests to know and delete permit the business 45 calendar days to comply (90 days at the most, under certain circumstances), a business must comply with a request to opt-out "as soon as feasibly possible, but no later than 15 business days from the date the business receives the request." One of the reasons for the difference in allotted time is that there is no requirement for the business to verify (make sure that the person making the request is legitimate) requests to opt-out. However, if a business cannot independently verify a request to know or delete, they can deny such requests without further inquiry.

III. Conclusion

Compliance under the CCPA begins with understanding the nature of the business and how it operates. The OAG's recent changes to the CCPA's regulations make clear that the goal of the statute is to increase the burden on larger organizations that handle consumers' personal information. However, particular characteristics, such as online presence or product offerings, may provide a way for those larger businesses to find ways to stay well within compliance, but ease the burden whenever possible.

**Karl Rumph is a law student intern in Morrison Mahoney's Cybersecurity, Data Privacy and Protection Practice*