ECKERT SEAMANS ATTORNEYS AT LAW

October 28, 2020

Data Security & Privacy Alert

California Privacy Rights Act of 2020 to Appear on November Ballot: Introduces Significant Amendments to CCPA

By Sandy B. Garfinkel & Stephenie G. A. Scialabba

A proposed privacy law known as the California Privacy Rights Act of 2020 ("CPRA") will officially appear for a referendum vote on the November 2020 ballot in California. If passed, the CPRA will expand upon what is already the most comprehensive consumer privacy law in the U.S., the California Consumer Privacy Act ("CCPA), introducing additional privacy obligations and concepts by amending the CCPA's scope, vendor provisions, individual rights, and enforcement measures.

Hanging in the balance is the establishment of a new administrative agency – the California Privacy Protection Agency ("CalPPA") – vested with investigatory and enforcement powers. With the CPRA's renewed focused on enforcement, and the proposed tripling of fines, businesses should pay close attention to the results of the referendum and begin thinking of how the following key provisions may affect operations:

REVISED "BUSINESS" DEFINITION:

- The CPRA raises one of the existing CCPA thresholds to qualify as a covered "Business" and makes minor changes to the "common branding" framework used to indirectly bring companies that would otherwise evade the scope of the CCPA within the arm of the statute. However, the CPRA does nothing to address the sought-after clarification on what it means to "do business" in the state. As a result, many companies are likely to continue voluntary compliance efforts out of fear that an online presence and availability to California residents may render them subject to the act.

THE RIGHT TO "RESTRICTION" & "CORRECTION:"

- Businesses need to be acutely aware of the types of information they use and hold about Consumers, as Consumers will have the right to limit both the use and disclosure of a new category of personal information – Sensitive Personal Information. Businesses will also be obligated to take commercially reasonable steps to update and correct inaccurate personal information.

EXPANDED RIGHT TO KNOW AND DELETE:

- Businesses will need to enhance the Notice at Collection and provide information on data retention to Consumers. Additionally, they will need to contend with an expanded right to know the purpose, content and recipients of personal information that is shared for certain types of advertising.

OVERHAULED CONTRACTING REQUIREMENTS:

- Just as companies begin to settle into their tailored Service Provider Agreements, the CPRA ushers in a new wrinkle by distinguishing between "Service Providers" and "Contractors," enhancing statutory contractual requirements, and extending those requirements to Third Party sales. As a result,

© Eckert Seamans Cherin & Mellott, LLC, 2020, all rights reserved.

businesses will need to revisit or execute agreements with any recipients of personal data to ensure that they satisfy the statute. Further, the CPRA seemingly limits the existing ability of Service Providers to sell information on behalf of a Business, placing companies with outsourced marketing back at square one.

NEW & EXTENDED STATUTORY EXCEPTIONS:

- Businesses that are focused more on the aggregate value of data need to take actions prescribed in the CPRA in order to qualify data as "de-identified," including public commitment to maintain information in the de-identified form and contractually requiring recipients to comply with various provisions of the CPRA.

- The operational relief that stems from the two-year extension of the "employee" and "business-to-business" (B2B) exemptions in place under the CCPA cannot be overstated. The exemptions will not sunset until January 1, 2023, and without this extension, Businesses would be forced to offer the full array of CCPA rights to employees, job applicants, pure business contacts, and others.

- Certain types of advertising and marketing will qualify under the "business purpose" exception to a "sale," further underscoring that the trumpeted right to "opt-out of advertising" is not as comprehensive as it may first appear. Additionally, under the CPRA, those companies indirectly receiving personal information at the direction of the Consumer are free to re-sell that personal information. This could prove to alleviate some roadblocks for the marketing and sales industry.

RESTRICTIONS ON THE USE OF "SENSITIVE PERSONAL INFORMATION:"

- Businesses will be restricted in the use of a new category of personal information, "Sensitive Personal Information," which includes a Social Security Number, driver's license, passport, financial account information, precise geolocation, race, ethnicity, religion, union membership, personal communications, genetic data, biometric or health information, and information concerning sex life or sexual orientation. If a Business intends to use this information for other purposes, or to infer characteristics about the Consumer, the Business will need to provide Consumers with an option to limit the use of the information similar to the right to "opt-out" of the sale (and/or share, under the CPRA) of non-sensitive information.

GDPR PROCESSING & SECURITY STANDARDS:

- The CPRA attempts to parallel the "reasonably necessary and proportionate" standard found in the European Union's General Data Protection Regulation ("GDPR"). The CPRA requires that *all* collection, retention, use and sharing of personal information be reasonably necessary and proportionate to the disclosed purposes of the same. As for Sensitive Personal Information, Consumers can restrict the processing of the information to that which is absolutely necessary for the provision of goods or services, rather than that which is reasonably necessary for a disclosed purpose.

- Security costs will be amplified under the CPRA, as Businesses whose processing of personal information presents a "significant risk" to Consumers' privacy will be required to conduct annual cybersecurity audits and submit risk assessments to CalPPA.

© Eckert Seamans Cherin & Mellott, LLC, 2020, all rights reserved.

EXPANDED PRIVATE RIGHT OF ACTION & TRIPLED FINES:

- Businesses face greater exposure for data breaches and violations under the CPRA. The private right of action for a data breach is expanded to cover the compromise of a Consumer's email address in combination with a password or security question and answer that would permit access to the Consumer's account. Additionally, the CPRA triples the CCPA's administrative fines for collecting and selling children's private information. In light of this, Businesses would do well to re-evaluate whether the value of maintaining high-risk categories of information outweighs the accompanying liability.

If approved by California voters in November, the majority of CPRA provisions will go into effect on January 1, 2023, with enforcement to begin July 1, 2023. The full text of the proposed initiative can be viewed here: Proposition 24, the California Privacy Rights Act (CPRA).

ECKERT SEAMANS ATTORNEYS AT LAW

This Data Security & Privacy Alert is intended to keep readers current on developments in the law. It is not intended to be legal advice. If you have any questions, please contact Sandy Garfinkel at 412.566.6868 or sgarfinkel@eckertseamans.com, or Stephenie Scialabba at 412.566.1925 or sscialabba@eckertseamans.com, or any other attorney at Eckert Seamans with whom you have been working.

© Eckert Seamans Cherin & Mellott, LLC, 2020, all rights reserved.