Alerts & Publications

The Group Behind the CCPA Aims to Strengthen it with a New Ballot Initiative

September 27, 2019

KEY CONTACTS

Melody Drummond Hansen
Silicon Valley
D: +1-650-473-2636

Randall W. Edwards
San Francisco
D: +1-415-984-8716

Scott W. Pink
Silicon Valley
D: +1-650-473-2629

Aleksander (Sasha) Danielyan
Silicon Valley
D: +1-650-473-2653

On September 25, 2019, Californians for Consumer Privacy, the nonprofit group behind what became the California Consumer Privacy Act enacted last year, filed a new ballot initiative, "The California Privacy Rights and Enforcement Act of 2020" (CPREA). The CPREA is intended to significantly revamp and strengthen the CCPA. If passed, the law would require California to establish a new data protection agency responsible for enforcing privacy violations and issuing new regulations. Specifically, it would add new restrictions or obligations, including opt-out rights regarding targeted advertising, opt-in requirements for the sale of sensitive information and duties for sensitive information, disclosure requirements for use of sensitive information for political purposes, an expanded definition of public information and a clarification of de-identified information, a new right of rectification, and greater protection of minors.

To be placed on the ballot for the November elections, the group will need to collect more than 620,000 signatures of registered California voters.

The CCPA, which the legislature extensively amended earlier this month and is not yet effective, is itself a significant expansion of privacy law, granting California consumers broad rights to control their personal information. Once effective, California's law will be the strictest in the nation and will impose significant new obligations on companies with respect to personal information of California residents. The final step is for the California Attorney General to issue regulations relating to the CCPA. The law takes effect on January 1, 2020, with enforcement delayed until six months after issuance of the Attorney General's regulations, or July 1, 2020, whichever is sooner.

Establishing the California Privacy Protection Agency

To strengthen enforcement of California's privacy laws, the CPREA proposes to establish a new regulatory body called the California Privacy Protection Agency (CPPA) (similar to data protection authorities under the GDPR). The CPPA would implement and enforce the CCPA and the CPREA through a variety of means, such as:

- Initiating administrative and civil enforcement actions;
- Adopting, amending, and rescinding California privacy regulations;
- Guiding companies on privacy compliance issues;
- Guiding consumers on their privacy rights; and
- Provide technical assistance and advice to the legislature regarding privacy-related legislation.

The Agency would have five members appointed by California's Attorney General, Senate President Pro Tem, Speaker of the Assembly, and the Governor. Members may not serve for longer than eight consecutive years. The Agency would then appoint an executive director, officers, counsel, and employees.

Additional Rights and Duties Regarding the Collection and Management of Sensitive Personal Information

The CPREA introduces the concept of "Sensitive Personal Information," defined as:

> "a consumer's social security, driver's license, state identification card, or passport number; a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; a consumer's precise geolocation; personal information revealing a consumer's racial or ethnic origin, religion, or union membership; the contents of a consumer's private communications, unless the business is the intended recipient of the communication; a consumer's biometric information; data concerning a consumer's health; data concerning a consumer's sexual orientation; or other data collected and analyzed for the purpose of identifying such information."

The CPREA would create new rights regarding Sensitive Personal Information, including:

- Opt-in for sale: requiring consumers to expressly opt-in to the sale of Sensitive Personal Information. This differs from the opt-out approach for other personal information defined in the CCPA.
- Opt-out for sale: requiring businesses to (1) provide notice to consumers that their sensitive personal

information may be used or disclosed to a service provider or contractor for advertising and marketing and that consumers have the right to opt-out of such use or disclosure; and (2) provide easily accessible tools for consumers to obtain their personal information, delete it, correct it, and opt-out of the sale of their personal information.
- Transparency: the CPREA would require new disclosures regarding the collection and use of Sensitive Personal Information, and limit businesses' use of the information to what was in disclosure.

Additionally, the CPREA would require transparency regarding automated decision-making processes that use Sensitive Personal Information.

New Right of Rectification

The CPREA would create a new right to require, upon request by a consumer, that a business use commercially reasonable efforts to correct inaccurate personal information the business maintains.

Businesses also would need to disclose to consumers their right to request correction of inaccurate personal information.

User of Personal Information for Political Purposes—New Rights to Know

Consumers will now have a right to request from a business the categories of person to whom that customer's personal information was disclosed for a business purpose. CPREA also gives consumers the right to request from a business details about information shared for political purposes, including names of candidates or organizations and uses to which the information was put.

Expanded Definition of Public Information

The term "personal information" still would exclude "publicly available" information as it does under the CCPA, but it now also would exclude de-identified information. The CPREA expands the definition of "publicly available" to include "information that a business has a reasonable basis to believe is lawfully made available to the general public from widely distributed media, or by the consumer, or by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience."

Clarification of What Is De-identified Data

The CPREA would clarify the definition of "de-identified" to mean information that cannot reasonably be used to infer information about, or otherwise be linked to, an identifiable consumer, provided that the business that possesses the information:

> (A) takes reasonable measures to ensure that the information cannot be associated with a consumer or household;
>
> (B) publicly commits to maintain and use the information in de-identified form and not to attempt to re-identify the information, except as necessary to ensure compliance with this subdivision; and
>
> (C) contractually obligates any recipients of the information to comply with all provisions of this subdivision.

New Definitions of Contractor and Service Provider

The CPREA would define the term "contractor" to mean a person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, so long as the contract contains (1) some outlined prohibitions relating to consumers' personal information and (2) a certification of the contractor's compliance with the prohibitions.

The term "service provider" would be expanded to now include:

- Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business; and
- Combining the personal information that the service provider receives from or on behalf of the business, with personal information from other sources.

Importantly, if a service provider engages another person to assist in performing a business purpose on behalf of the business, the service provider must notify the business and contract with the other person to observe all the requirements in the definition of a "service provider."

Clarification of Business Purposes

"Business Purpose" is clarified to mean the use of personal information for the business's or service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed.

Specific business purposes are enumerated, such as auditing relating to the interaction with the user, debugging, verification, quality or safety assessment, short-term transient use, performance of services on behalf of the business or service provider, and internal research for technological development and demonstration.

Greater Protection of Minors

Among a few increased privacy protections for minors, the CPREA triples CCPA's fines for violations governing the collection and sale of children's private information. It also requires opt-in consent to collect data from consumers under the age of 16.

Amending Process

California is one of 24 states that have ballot initiatives. In California, for an initiative to appear on the ballot, the sponsors need to obtain the signatures of five percent of the total gubernatorial vote in the most recent election. Under California law, ballot initiatives can only be amended through a separate popular vote and not through the legislative process—a drawback of the initiative process.

The CPREA is designed to be amended through a majority vote in the California Legislature, however, so long as the amendments are consistent with and further the purpose and intent of the CPREA.

Next Steps

The goal of Californians for Consumer Privacy is to obtain enough signatures for the CPREA to be put on the November 2020 ballot. If passed, the CPREA will become effective on January 1, 2021, but will only be applicable to personal information collected by a business on or after January 1, 2020, the date the CCPA will become effective.

This memorandum is a summary for general information and discussion only and may be considered an advertisement for certain purposes. It is not a full analysis of the matters presented, may not be relied upon as legal advice, and does not purport to represent the views of our clients or the Firm. Melody Drummond Hansen, an O'Melveny partner licensed to practice law in California, Washington, DC, and Illinois, Randall W. Edwards, an O'Melveny partner licensed to practice law in California, Scott Pink, an O'Melveny special counsel licensed to practice law in California, Amit Itai, an O'Melveny associate licensed to practice law in Israel, and Aleksander (Sasha) Danielyan, an O'Melveny staff attorney licensed to practice law in California, contributed to the content of this newsletter. The views expressed in this newsletter are the views of the authors except as otherwise noted.

© 2019 O'Melveny & Myers LLP. All Rights Reserved. Portions of this communication may contain attorney advertising. Prior results do not guarantee a similar outcome. Please direct all inquiries regarding New York's Rules of Professional Conduct to O'Melveny & Myers LLP, Times Square Tower, 7 Times Square, New York, NY, 10036, T: +1 212 326 2000.