O'Melveny

Alerts & Publications

Voter-Approved Privacy Law Could Mean Big Changes for Big Tech

November 9, 2020

KEY CONTACTS

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

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

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

Find more alerts and insights for emerging and tech companies at omm.com/momentum.

The California Privacy Rights Act (CPRA), which voters approved last Tuesday, November 3, could have profound consequences for data-dependent businesses, changing how businesses collect, share, and sell California consumers' personal information and establishing a new watchdog for consumer privacy in California. Although the CPRA does not take effect until January 1, 2023, covered businesses should begin now to evaluate the significant changes that the law brings.

The CPRA makes significant changes to the existing California Consumer Privacy Act (CCPA): creating a first-of-its-kind state data-protection agency, adding new consumer rights to control use and sharing of information, creating new retention obligations, increasing penalties for violating rights of minors, and clarifying the roles and responsibilities of contractors and service providers. It also includes some provisions favorable to businesses, such as extending the employee and business-to-business exemptions under the CCPA to January 1, 2023, and expanding the definition of what is publicly available information exempt from the law.

Until the CPRA goes into effect in 2023, covered businesses must comply with the current version of the CCPA and the Attorney General Regulations while at the same time preparing to comply with the CPRA.

The CPRA makes the following key changes to the CCPA:

- Establishes the California Privacy Protection Agency.
  - The agency will be led by five appointed members and tasked with developing regulations on various CCPA and privacy topics;
  - The agency will have the power to enforce the CCPA, seek injunctive relief, and impose civil penalties of up to $2,500 per violation and up to $7,500 for intentional violations;
  - Unlike European data-protection authorities, the agency will have broader discretionary power, including the ability to

start investigations and initiate administrative actions, provide privacy guidance to consumers and businesses, and promote public awareness of privacy rights and risks, among others duties. But, the agency must stay any administrative action if the Attorney General proceeds with enforcing a given investigation or civil action under the CCPA, including as amended by the CPRA.

- Creates additional consumer rights, including:
  - The right to request that a business correct inaccurate personal information that the business maintains. This is similar to the right of rectification under Article 16 of the GDPR.
  - The right to control use and sharing of sensitive personal information.
    - Under the CCPA, "sensitive personal information" covers a broad set of data, including personal identification numbers (such as Social Security Numbers), financial account information (such as credit card number) that would enable access to the account, precise geolocation (i.e., data locating a consumer within 1,850 feet), content of mail, emails, and texts unless the business is the intended recipient, racial or ethnic origin, religious or philosophical beliefs, or union membership, genetic data, biometric information, health information, and information concerning a consumer's sex life or sexual orientation.
    - Among other requirements, businesses must provide consumers with a conspicuous link titled, "Limit the Use of My Sensitive Personal Information," unless consumers have the ability to opt-out through an opt-out preference signal sent with the consumer's consent.
    - Consumers may restrict the disclosure and use of sensitive personal information except as "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods and services."
- The expansion of the opt-out right to both selling and "sharing" information.
  - Businesses must now give consumers the ability to opt out of sharing of personal information.
  - Opt-out links must be revised to read, "Do Not Sell or Share My Personal Information," unless consumers have the ability

to opt out through an out-out preference signal sent with the consumer's consent.
    - The CPRA broadly defines "sharing" as "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means."
- The right to opt-out of "cross-context behavioral advertising."
    - The CPRA defines "cross-context behavioral advertising" as the targeting of advertising to a consumer based on personal information obtained from the consumer's activity across businesses, distinctly branded websites, applications, or services other than the business, website, application, or service with which the consumer intentionally interacts.
    - The CPRA includes cross-context behavioral advertising in the definition of "sharing" and excludes it from the definition of "business purpose" for the collection and use of personal information, resolving the potential ambiguity of whether data sharing for certain advertising purposes constitutes a "sale" under the CCPA.
    - The CPRA also provides that service provider or contractor that provides advertising and marketing services to a business cannot combine the personal information of opted-out consumers of the business with personal information that the service provider or contractor receives from or on behalf of another person or persons, or collects from its own interaction with consumers. This could require advertising technology companies and publishers to take additional steps to segregate data.
    - Businesses will have to provide consumers the right to opt-out from the collection of ad cookies by third parties if used for this type of advertising. This new right may have profound consequences for the advertising technology sector.

- Changes the criteria defining businesses subject to the CCPA.
    - The CCPA applies to businesses that operate in California and meet one of three thresholds. The CPRA changes or clarifies each of these thresholds.
        - Gross revenue: The first $25 million annual gross revenue threshold will be determined as of January 1 of the calendar year based on the gross revenues for the preceding calendar year;

    - Number of consumers or households: Increases the threshold from 50,000 to 100,000, no longer applies to "devices," and applies only to the number of consumers and households whose personal information a business "buys, sells or shares" annually, not what a business "receives." This change could narrow the application of this threshold.
    - Percentage of revenue from selling personal information: Now applies to businesses that derive at least half of their revenue from selling or sharing personal information, rather than from selling only.

- The CPRA clarifies and expands the situations where affiliated businesses might be considered part of the same "business" and subject to the CCPA.
    - Under existing law, an affiliated business includes an entity that controls or is controlled by a business and that shares common branding with the business.
    - The CPRA adds the requirement that to be considered part of the same business, the business must share consumers' personal information with the other entity.
    - The CRPA's definition of an affiliated business now includes a joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. The joint venture or partnership and each owner or partner business shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.

- Expands the definition of publicly available information that is exempt from the CCPA requirements.

- The CPRA expands this exemption to include not only information from government records, but information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer, by widely distributed media, or by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.
    - This would mean, for example, that if a consumer publicly posts their e-mail address on social media, that e-mail address would be exempt from the CCPA.
    - The expanded definition also exempts lawfully obtained information and truthful information that is a matter of public

concern -- changes designed to address the use of information for journalistic purposes.

- Clarifies that CCPA does not prohibit loyalty, rewards, premium features, discounts, or club card programs.
    - This change addresses questions about whether the CCPA's right to non-discrimination prohibited offering loyalty programs that require the collection of personal information.
- Triples the penalty threshold to $7,500 per violation for violations relating to consumers younger than 16.
- Clarifies the roles of businesses and their contractors and service providers.
- The CPRA creates a new category of "contractors" that are parties to whom a business makes available a consumer's personal information for a business purpose as defined in the law pursuant to a written contract with the business. A service provider is a party that processes personal information on behalf of a business for a business purpose pursuant to a written contract, provided that the contract prohibits the service provider from reselling the personal information or retaining or using the information outside of the business purposes and the relationship with the business. The difference is that a disclosure to service provider is not a sale if certain conditions are met whereas a disclosure to a contractor could be a sale to which the opt-out rules apply.
    - The CPRA requires businesses that sell, share, or disclose personal information with contractors, service providers, and third parties must enter into contracts that contain certain compliance requirements, including using the information for limited and specified purposes; complying with and providing the same level of privacy protection as the CPRA, and granting the business certain rights to ensure compliance. In turn, service providers must have similar contracts with the sub-service providers. This will require companies to revisit all of their vendor and service provider agreements.
    - The act includes provisions that clarify the responsibilities of businesses and contractors and service providers in responding to consumer data requests.
    - The act requires contractors to certify that they understand and will comply with contractual restrictions and that they

are not explicitly obligated to process personal information on behalf of a business.
    - The act clarifies that service providers cannot combine personal information they collect as service providers with information either collected in their "business" capacity or received from other businesses.

- Imposes additional obligations on businesses to manage personal information they collect from consumers.

- The CPRA requires businesses to notify consumers of the length of time for which they plan to retain each category of personal information.
    - Businesses cannot retain personal information longer than is "reasonably necessary" for the collection's disclosed purposes.
- The CPRA requires businesses to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal Information from unauthorized or illegal access, destruction, use, modification, or disclosure.
- The CPRA adopts a definition of consent that is similar to the definition under the GDPR.
    - Consent must be "freely given, specific, informed and unambiguous" and must define the purpose of the particular processing to which the consumer is consenting.
    - This new definition may require consideration of whether the current use of checkboxes is sufficient to meet consent requirements. This will need to be clarified in future rulemaking.
    - Acceptance of general or broad terms of use or hovering over, muting, pausing, or closing a given piece of content does not constitute consent.
    - The act also clarifies that an agreement obtained through use of "dark patterns" does not constitute consent. The CPRA defines "dark patterns" as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice." This definition will likely be widely interpreted and may need to be clarified in future rulemaking.

For more information on the regulations, and CCPA compliance, please see our prior alerts and our CCPA toolkit.

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. Randall W. Edwards, an O'Melveny Partner licensed to practice law in California, Scott W. Pink, an O'Melveny Special Counsel licensed to practice law in California, 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.

© 2020 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.