November 29, 2020

CLIENT ALERT

The California Privacy Rights Act (CPRA) Amends the California Consumer Privacy Act (CCPA)

Less than a year after the groundbreaking California Consumer Privacy Act (CCPA) entered into effect, and less than six months after it became enforceable, California is enacting the California Privacy Rights Act (CPRA) which introduces major changes to the CCPA. The CPRA's enactment is performed through a procedure unique to California, where the voters of California directly approve a legislative ballot initiative.

While organizations have dedicated efforts in the past two years to come into compliance with the CCPA, the CPRA, with its phased roll-out between 2021 and 2023, will bring about dozens of additional GDPR-inspired obligations, yet will introduce few reliefs for businesses. Most of the CPRA's far-reaching amendments will become effective in 2023.

Changes Effective in 2021

The California Privacy Protection Agency. The CPRA brings a significant institutional change with the establishment of the California Privacy Protection Agency (the "Agency"). The Agency will be vested with full administrative power to implement and enforce the CPRA and promote public awareness of consumer privacy. By July 1, 2021, the Agency will assume the rulemaking responsibility that is currently vested with the California Attorney General.

Extension of Exemptions. The CCPA provided that for the period through December 31, 2021, most of the CCPA's obligations would not apply to personal information that a business collects about its employees, job applicants, or freelancers. A similar provision was also enacted for personal information that a business processes when it liaises with a representative of another organization in a Business-to-Business transaction. The CPRA will extend these exemptions for an additional year, until December 31, 2022, and they will fully expire on January 1, 2023.

Changes Effective in 2022

New Regulations. The CPRA requires that the Agency adopt new rules and procedures for businesses on a variety of topics by July 1, 2022. Businesses will then have a grace period of at least one year until these new regulations become enforceable against them on July 1, 2023. The topics on which the Agency must implement regulations include:

- Annually required cybersecurity audits when a business's processing of consumers' personal information presents a significant risk to privacy or security;
- A privacy risk assessment that businesses will be required to periodically file with the Agency, to restrict of prohibit their processing if the risks to consumer privacy outweigh the benefits resulting from processing;

- Consumers' access and opt-out rights concerning businesses' use of automated decision-making technology, including meaningful information about the logic involved in such decision-making and a description of its consequences;
- The scope and process of the Agency's audit authority over businesses;
- A business's permissible uses and disclosures of a consumers' sensitive personal information; and
- Instructions on mechanisms that businesses will be required to implement for consumers to be able to exercise their right to opt-out of the sale or sharing of their personal information.

Look-back Window. Generally, the CPRA's new obligations (which take effect in 2023) apply to personal information that a business will have collected on or after January 1, 2022. Also, the CPRA will extend the consumers' right to request information about a business's past processing of personal information, beyond just the CCPA's 12-month window that precedes the consumer's requests. Yet, a business's obligation to provide such extended look-back information will only apply to personal information that a business will have collected on or after January 1, 2022.

Changes Effective in 2023

The bulk of the CPRA's amendments will become effective on January 1, 2023, with some of the key ones described below.

Scope of Applicability. The CPRA introduces key amendments to the threshold criteria for the law's applicability to businesses. First, the CPRA would apply to any business that annually processes the personal information of 100,000 Californians (compared to 50,000 under the CCPA). Second, the CPRA would apply to any business that derives half or more of its annual revenue from "selling" personal information (as the CCPA currently provides) or from sharing personal information (with or without charge) with a third party for online behaviorally-targeted ads.

Also, unlike the CCPA, which applies to all corporate group affiliates of a business subject to the CCPA if they share common branding, the CPRA will only apply to such corporate group affiliates if the business shares personal information (with or without charge) to them for behaviorally-targeted ads.

Publicly Available Information is not Subject to the CPRA. The CPRA's obligations on businesses, and the privacy rights it gives consumers, will not apply to information that a business reasonably believes is lawfully made available to the general public by the consumer or from widely distributed media. This carve-out likely will allow companies to harvest personal information that is publicly posted on social networks, without being subject to any CPRA obligations with respect to such harvested data.

Limitations on Processing. The CPRA includes a new, overarching obligation on businesses' collection, use, retention, and sharing of a consumer's personal information. The collection and processing must be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected. Personal information may not be further processed in a manner that is incompatible with those purposes and may not be retained for longer than is reasonably necessary for the disclosed purpose of its collection and processing.

Behaviorally-targeted Ads. The CPRA explicitly specifies consumers' rights to opt-out of having their personal information disclosed to third parties, such as ad networks, for online behaviorally-targeted ads.

Sensitive Personal Information. The CPRA creates a new category of "sensitive" information that includes government-issued identifiers (e.g., Social Security Numbers, driver's license number or passport number), online account or financial account credentials, precise geolocation, racial or ethnic origin, religious beliefs, contents of the consumer's email or text messages, health information, genetic data, biometric information, and information about the consumer's sex life or sexual orientation.

The CPRA grants consumers the right to instruct a business to limit its use of the consumer's sensitive information only as necessary and reasonably expected to perform the services or provide the goods requested. A business must provide a clear and conspicuous link on the business's homepage, titled "Limit the Use of My Sensitive Personal Information", that enables a consumer to exercise this right.

Disclosures of Personal Information to Others. The CPRA imposes additional contractual requirements on businesses that sell or merely disclose personal information to service providers, contractors, or any other third parties. Businesses must enter into a written contract with such parties, which among other matters:

- Specifies that the information may only be used for the limited purposes specified in the contract;
- Requires the recipient to comply with the CPRA and provide the same level of privacy protection;
- Requires the recipient to notify the business if it can no longer meet its CPRA's obligations;
- Allows the business to take reasonable steps to help ensure that the recipient uses the information in a manner consistent with the business's obligations under the CPRA; and
- Allows the business to take reasonable steps to stop and remediate unauthorized use of the information.

End Notes

These developments likely warrant review, adjustments, and changes in companies' front-end and back-end privacy practices ahead of the CPRA's effective date in 2023. We therefore recommend that organizations pencil a CPRA compliance project into their business plans for 2022.

Ariel Amir

AAmir@PearlCohen.com

Dotan Hammer

DHammer@PearlCohen.com

Internet, Cyber and Copyright Group
Pearl Cohen Zedek Latzer Baratz