California Privacy Rights Act

Malk Insights — April 2023

Key takeaways

- The CPRA amends the existing CCPA by providing California consumers and employees with additional rights to correct and limit the use and disclosure of sensitive personal information collected and processed by businesses
- All provisions of the CCPA are still currently in effect and enforceable, with enforcement of the supplemental CPRA beginning in July 2023
- The CPRA update reflects increased regulatory scrutiny over the consumer data privacy and security practices of businesses in California, with similar laws beginning to be enacted in other states

Overview of the CPRA and CCPA

The California Privacy Rights Act (CPRA), also known as Proposition 24, is a ballot measure approved at the end of 2020 and effective January 1st, 2023. The CPRA is an amendment of the existing California Consumer Privacy Act (CCPA) which provides consumers in California more control over the personal information that businesses collect about them.

What is the CCPA and to whom does the regulation apply?

The CCPA is a 2018 regulation that initially created four privacy rights for consumers in California, including:

- The right to know about the personal information a business collects about them, from whom it is collected, the reasons for collection, and how it is used, shared, and/or sold (if applicable)
- The right to delete personal information collected from them (with some exceptions)
- The right to opt-out of the sale or sharing of personal information (opt-in for those under the age of 16)
- The right to non-discrimination in treatment for exercising CCPA rights

The CCPA imposes obligations on companies doing business in California, as well as any service providers or third parties to which personal information is shared or sold by those businesses, respectively. The CCPA applies to businesses with any one of the following characteristics:

- Businesses generating over $25M in annual revenue in California
- Businesses processing the personal information of over 100K California consumers
- Businesses deriving >50% of annual revenue from selling of California consumer personal information

Service providers processing consumer personal information (i.e, information that identifies, relates to, or could reasonably be linked with a consumer, such as name, email address, records of products purchased, internet browsing history, and any sensitive personal information defined under the CPRA) on behalf of businesses must use personal information only for specified purposes, implement security safeguards, ensure personal information is segregated between engaged businesses, and notify businesses of subcontractor usage/ensure safeguards. Meanwhile, third parties must not resell consumer personal information sold to them without explicit notice and opportunity to opt out to the consumer.

Businesses subject to the CCPA have several responsibilities, including responding to California consumer requests to exercise these rights, giving consumers certain notices explaining their privacy practices, and implementing security safeguards. Businesses can process user opt-out requests via industry tool, global privacy control (GPC). Under limited circumstances, consumers also have the right to initiate a private cause of action for data breaches should their nonencrypted, nonredacted personal information be stolen as a result of a business' failure to maintain reasonable security practices to protect the data. Before suing, consumers must give the business written notice of which CCPA sections have been violated and allow 30 days to respond in writing that it has cured the violations with no further violations.

Notably, the CCPA defines the 'sale' of personal information as the selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration. However, the CCPA had not defined the 'sharing' of information.

Furthermore, the CCPA had contained an employee and business-to-business (B2B) exemption for personal information collected by a business about past, potential, or current employees (including owners, directors, officers, contractors, and beneficiaries/dependents) and business contacts, respectively—which expired on January 1st, 2023. The exemption was limited to when businesses used employee personal information solely for employment-related actions (e.g., recruitment, payroll functions), or when businesses used employee or business contact personal information to support the provision or receipt of a product/service to or from other businesses.

How does the CPRA amend the CCPA?

The CPRA became effective on January 1st 2023, though enforcement action will not formally begin until July 1st, 2023 and will only apply to CPRA violations occurring after that date. Notably, however, the CCPA's provisions still remain in effect and are currently enforceable as well.

The CPRA newly creates the California Privacy Protection Agency (the "Agency") to implement and enforce the CCPA, as amended by the CPRA. In the future, the Agency will further define enforcement items under the CCPA. Although the Agency has fully authority to implement and enforce the CCPA, the California Attorney General still retains enforcement powers as well. The CPRA also grants consumers with two additional privacy rights:

- The right to correct inaccurate personal information that a business has about them
- The right to limit the use and disclosure of sensitive personal information

Under the CPRA, sensitive personal information is a newly defined category within the existing definition of personal information for which consumers can limit the use and disclosure of by businesses. A consumer's sensitive personal information includes:

- Social security, driver's license, state identification card, or passport number
- Account log-in and credentials (e.g., access code), financial account, and PCI information
- Racial/ethnic origin, religious or philosophical beliefs, and union membership
- Contents of mail, email, or messages (unless the business is the intended recipient)
- Precise geolocation (within a radius of 1,850 feet)
- Genetic or biometric information (e.g., fingerprints)

Unlike the CCPA, the CPRA defines the 'sharing' of personal information as the renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating consumer personal information by business to a 3rd party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

The CPRA also eliminates the 30-day cure period originally permitted under the CCPA, as the Agency can choose not to investigate a complaint or provide a business with a time period to cure the alleged violation on a discretionary basis, taking into consideration the lack of intent to violate the CCPA or voluntary efforts undertaken by the business to cure the alleged violation prior to being notified by the Agency of the complaint.

Furthermore, the CPRA establishes contractors as a fourth entity in addition to businesses, service provides, and third parties which collect and/or process personal information. Contractors are people to whom the business makes available consumers' personal information for business purposes but are never the recipient of a 'sale' or 'sharing' of personal information. Still, they are bound by terms of a written contract which stipulates restrictions on the use of personal information, and they must certify their understanding and compliance with restrictions.

Finally, the CPRA does not contain a provision to extend the partial employee and B2B exemptions provided under the original CCPA, meaning that businesses will now have obligations under the CCPA regarding the employee and business contact personal information that they collect—as employees and business contacts will be afforded the same data privacy rights as consumers under the CCPA.

ESG implications of the CPRA amendment

The CPRA amends the CCPA to provide additional consumer privacy rights and clarify business obligations under the privacy regulation. The amendment represents increased regulatory scrutiny of California business' data privacy and security practices, and a commitment towards enforcing the CCPA.

Indeed, the California AG declared its first public enforcement action under the CCPA in August 2022, requiring beauty retailer Sephora to pay a $1.2M settlement after conducting an enforcement sweep of online retailers. The AG alleged that Sephora failed to disclose to consumers that it was selling their personal information and provide the right to opt out through two or more methods, and that it failed to process user requests to opt out of the sale via GPC in violation of the CCPA. Furthermore, Sephora failed to cure these violations within the 30-day period allowed under the CCPA after notification by the AG. Under the CPRA, businesses may not have a cure period to rectify identified violations, and firms will thus be further held accountable to future CCPA violations.

Furthermore, because the CPRA has not extended the partial employee and B2B exemptions of the original CCPA, California employers must ensure that their CCPA privacy notices provided to employees are updated

to describe and explain how employees can submit requests under their new CCPA privacy rights. Businesses must also enter into data processing agreements with service providers with which employee and business contact personal information is shared, else the sharing of this personal information may constitute a 'sale' which triggers opt out rights for employees.

Similar to the CCPA update, state regulators across the United States are also increasingly scrutinizing the consumer data privacy and security practices of businesses, as novel laws such as the Colorado Privacy Act, Connecticut Data Privacy Act, Utah Consumer Privacy Act, Virginia Consumer Data Protection Act coming into effect in 2023 to provide consumers with similar rights. Moving forward, companies should re-evaluate their compliance with the CCPA and other similar privacy laws moving forward—ensuring GPCs are in place, maintaining consumer- and employee-facing disclosures and notices, and being prepared to honor consumer and employee rights.

Resources:

1. https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/
2. https://www.adlawaccess.com/2021/06/articles/cpra-update-what-is-a-contractor/
3. https://www.jdsupra.com/legalnews/data-privacy-faq-s-how-do-cure-periods-5265007/
4. https://www.jdsupra.com/legalnews/ccpa-enforcement-the-sephora-settlement-3993318/

Authors

Anastassia Bougakova
Senior Vice President
e: abougakova@malk.com

Storm McLaughlin
Engagement Manager
e: smclaughlin@malk.com

Ryan Kim
Senior Associate
e: rkim@malk.com

About Malk Partners

Malk Partners is the preeminent advisor to private market investors for creating and protecting value through environmental, social, and governance ("ESG") management and impact investing. Founded in 2009, Malk Partners advises many of the world's leading alternatives managers investing across private equity, growth equity, venture capital, and private credit by helping them define ESG goals, achieve ESG results, and guide their portfolio companies in driving value creation and mitigating risks. The firm is headquartered in La Jolla, California with a second office located in New York. For more information about Malk Partners, please visit www.malk.com.