SAUL EWING ARNSTEIN & LEHR LLP

ALERT

Cybersecurity and Privacy Practice

NOVEMBER 2020

The California Privacy Rights Act of 2020: How to Comply with the Newest Privacy Law

Alexander (Sandy) R. Bilus

On November 3, 2020, Californians went to the polls and voted in favor of making sweeping changes to their existing state privacy law. Proposition 24, known as the California Privacy Rights Act of 2020 ("CPRA"), modifies and expands on the California Consumer Privacy Act of 2018 ("CCPA"). The CPRA creates new and expanded rights for California residents and new compliance obligations for businesses. It creates a new agency, the California Privacy Protection Agency, that is tasked with implementing regulations and conducting investigations and enforcement actions. This article explains the key aspects of the CPRA and provides recommendations for how to go about complying with the law.

Does the CPRA Apply to Your Company?

First, you will need to determine whether the CPRA applies to your company. The CPRA applies to any for-profit entity that does business in California, collects and uses the personal information of Californians, and either (a) has annual gross revenues of at least $25 mm in the preceding calendar year, (b) buys, sells, or shares the personal information of at least 100,000 California residents or households, or (c) derives at least 50% of its revenue from selling or sharing personal information.

The CPRA also can apply if your company is a contractor or service provider for a business that is covered by the CPRA and it collects or uses personal information as part of providing those services to the business, or if your company buys personal information from a business or receives that information for cross-context behavioral advertising purposes.

New and Expanded Obligations on Businesses

- Previously, the CCPA required businesses to provide California residents with a notice at or before collection of their personal information that explained certain information about how the business intended to use their information. After the CPRA becomes effective, this initial notice must include: (1) the categories of personal information collected about the individual; (2) the purposes for the collection or use of that information; (3) whether the business sells or shares the personal information; (4) the categories of "sensitive" personal information; (5) the purposes for the collection or use of that sensitive information; and (6) whether the business sells or shares that sensitive information.

- The CPRA includes a new limitation on all personal information processing: any collection, use, retention, or sharing of personal information must be "reasonably necessary and proportionate" to achieve the purposes for which the information was collected.

- The CPRA mandates that whenever a business discloses personal information to contractors or service providers, or sells or shares personal information to any third parties, the business executes an agreement with those entities that specifies, among other things, that the purposes of the disclosure obligates the counterparty to comply with the CPRA, grants the business the right to take "reasonably and appropriate steps" to ensure compliance by the counterparty, and requires the counterparty to notify the business if it can no longer comply.

- The CPRA requires businesses to implement "reasonable security procedures and practices" appropriate to the nature of the personal information to protect the information against a breach or loss.

- The CPRA expands on the CCPA's requirements for privacy policies, which now must describe the rights of Californians under the law and list the categories of personal information collected, the categories of the sources of personal information, the categories of the entities to whom the business will disclose the personal information, the categories of personal information

that the business sells or shares, and the categories of personal information that the business discloses for a business purpose.

New and Expanded Rights for California Residents

- The CCPA included a right to request deletion of personal information along with reasons why a business could refuse such a request. The CPRA modifies some of those reasons for rejecting requests. For instance, previously, a business could reject a deletion request if the personal information was necessary to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity. Now, a business can refuse a request if the information is "reasonably" necessary to help to ensure security and integrity to the extent the use of the personal information is "reasonably necessary and proportionate" for those purposes. Previously, a business could reject a request if it wanted to use the personal information "internally, in a lawful manner that is compatible with that context in which the consumer provided the information." Now, a business can no longer refuse a request on that basis.
- The CPRA adds a new right to request correction of inaccurate personal information. Businesses must take "commercially reasonable efforts" to correct inaccurate information in response to verified requests.
- Like the CCPA, the CPRA gives Californians the right to request information about how their personal information is being used by a business. The CPRA expands this right to require businesses to explain whether they are "sharing" personal information; i.e., whether they are disclosing personal information to third parties for cross-context behavioral advertising purposes.
- The CPRA allows Californians to opt out of the sale or sharing of their personal information.
- The CPRA give Californians the right to limit a business' use and disclosure of their sensitive personal information.
- Finally, like the CCPA, the CPRA provides that businesses cannot retaliate against individuals who opt out or exercise their CPRA rights.

How to Comply with the CPRA

If the CPRA applies to your business, you should consider taking the following steps to comply. First, create a "data inventory" that catalogs the sources of personal information collected or used by the business, the categories of personal information, the purposes of the collection, any entities to which your business discloses the personal information, the retention period or criteria used to determine the retention period for the information, and the security measures applied to protect the personal information. From here, your business can create and/or update its privacy notices and privacy policies so that they accurately describe the company's practices with respect to the personal information. Consider how your company will deliver those notices to individuals, depending on how they are interacting with your company – via a website, app, by email, in person, or on the phone. Review your existing contracts with third parties, contractors, and service providers to which your company discloses personal information to determine whether they need to include certain provisions required by the CPRA. Create or update any internal policies or handbook that describe how the company's employees should handle and respond to individuals when they seek to exercise their privacy rights. Finally, consider updating your training and auditing programs to ensure that your company's employees know how to comply and that the company redresses any compliance gaps going forward.

The CPRA becomes effective on January 1, 2023, and enforcement will begin on July 1, 2023. Although that may seem like a long time away, it should be evident that compliance with the CPRA is no easy task. The time to complete the compliance process is ticking. Saul Ewing Arnstein & Lehr LLP attorneys can help provide legal advice for your company as it seeks to comply with this new law. For more information, contact the author of this article.

This alert was written by Alexander R. Bilus, vice-chair of the Firm's Cybersecurity and Privacy Practice. Alexander can be reached at (215) 972-7177 or at Alexander.Bilus@saul.com. This alert has been prepared for information purposes only.

Did you find this information useful? Please provide your feedback here and also let us know if there are other legal topics of interest to you.