HINSHAW

What You Need to Know About California's New Voter-Approved California Privacy Rights Act

Hinshaw Alert | 3 min read
Dec 15, 2020

With the ink barely dry on the newly enacted California Consumer Privacy Act (CCPA), California voters have approved The California Privacy Rights Act (CPRA), which significantly amends the CCPA and creates new obligations for covered businesses. While not fully operative until January 2023 and not enforceable until July 2023, CPRA will require organizations currently grappling with CCPA compliance to further strengthen their data collection and privacy practices. CPRA builds on the CCPA, expanding consumer rights over their personal information and clarifying responsibilities for businesses that use such information. CPRA also imposes protections similar to those of the European Union's General Data Protection Regulation (GDPR), a reflection of where U.S. privacy regulation may ultimately be headed.

Noteworthy CPRA Requirements

- **Establishment of the California Privacy Protection Agency (CPPA)**. CPRA establishes and funds a first-of-its-kind state agency dedicated to privacy. The CPPA will be governed by a five-member board likely chosen in the next few months from among Californians with expertise in the areas of privacy, technology, and consumer rights. The agency will ultimately implement and enforce consumer privacy via administrative proceedings and fines between $2,500 and $7,500 per violation. Among other things, the agency will assume rule-making responsibilities and have the power to conduct audits of businesses to ensure compliance. The creation of this first-in-the-nation privacy agency is likely to lead to robust enforcement of the CPRA.
- **No Right to Cure**. CPRA eliminates the CCPA's right to cure an alleged violation within 30 days of notice of such allegation.
- **New Right of Correction**. CPRA adds an additional right for California consumers to correct inaccurate personal information.
- **New Category of Personal Information**. CPRA restricts the collection, use and disclosure of Sensitive Personal Information (SPI) which includes personal information that reveals government identification numbers, financial information, a consumer's precise geolocation, racial or ethnic origin, the contents of certain

consumer personal communications, and genetic data. Businesses will be required to provide consumers an opportunity to restrict or limit the use of SPI via a website opt-out link or opt-out preference signal.

- **Expanded Opt-Outs**. CPRA expands the CCPA's "opt-out of sale" rights to include "opt-out of sale and sharing" of personal information. "Sharing" includes the transferring or making available personal information to a third party "for cross-context behavioral advertising, whether or not for monetary or other valuable consideration." CPRA defines "cross-context behavioral advertising" as the "targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application or service with which the consumer intentionally interacts." In addition, CPRA provides consumers with opt-out rights with respect to a business's use of automated-decision making technology, including profiling. Businesses will be required to provide consumers meaningful information about the logic involved and the likely outcome of such decision-making.
- **Risk Assessments and Cybersecurity Audits**. CPRA requires businesses to conduct and submit to the CPPA risk assessments about whether the benefits of their processing of personal information outweighs the risks to consumer privacy. Businesses will be required to perform annual cybersecurity audits.
- **Purpose Limitation, Data Minimization and Storage**. CPRA will only permit businesses to collect personal information for "specific, explicit, and legitimate disclosed purposes" and "only to the extent that it is relevant and limited to what is necessary in relation to the purposes for which it is being collected, used and shared." CPRA requires businesses to disclose of "the length of time the business intends to retain each category of personal information or, if that is not possible, the criteria used to determine such period."
- **Service Providers and Contractors**. CPRA requires businesses that sell, share, or disclose personal information to enter into agreements prohibiting service providers, contractors (and their subcontractors) from, among other things, using or disclosing personal information for any purpose other than the business purposes specified.
- **Lookback Period**. Despite its January 2023 effective date, CPRA contains an expanded lookback period for information collected after January 1, 2022.

Takeaways

Businesses subject to the CPRA should begin the process of reviewing their privacy and cybersecurity policies and procedures in light of the new requirements imposed by the new law. They also should update their data maps and inventories to identify SPI and operationalize their obligations concerning that new category of personal information. Business also should review and update their service provider contracts to incorporate provisions required by CPRA.

Related Capabilities

Data Privacy, AI & Cybersecurity