wiley

NEWSLETTER

California Privacy Law on the Ballot: What to Expect on California's Upcoming Ballot Initiative to Expand and Amend the CCPA

October 2020

Privacy in Focus®

Next month, California voters will cast their votes on Proposition 24, a ballot initiative that, if passed, will enact the California Privacy Rights and Enforcement Act of 2020 (CPRA). The CPRA would significantly amend the California Consumer Privacy Act (CCPA) and would require businesses to once again re-examine their privacy compliance programs for California consumers.

The CPRA Envisions an Expanded Privacy Framework

The CPRA – which, if passed, would take effect on January 1, 2023 – spells out significant changes to the CCPA privacy framework. While consumer groups are divided in terms of their support for the ballot measure, the CPRA would require businesses to make further changes to their privacy and data governance practices.

Key provisions include:

Establishing New Privacy Enforcement Agency. The new law would create a new state agency – the California Privacy Protection Agency (the Agency) – to implement and enforce the CPRA. The Agency would be initially funded with $5 million in 2020-2021, and $10 million each year to follow. It would be governed by a five-member board of experts in privacy, technology, and consumer rights.

Expanding Consumer Opt-Out Right. The law would create a new definition of "sharing" as disclosing personal information to a third party for "cross-context behavioral advertising." The CPRA would

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

State Privacy Laws

establish similar business obligations for "sharing" information as the CCPA does for "selling" information, including the obligation to observe a consumer's right to opt out of the sharing of their data.

Aligning with GDPR Requirements. The CPRA would bring California law closer in line with the European Union's General Data Protection Regulation (GDPR) in several respects, including by implementing an overarching data minimization provision that requires the collection, use, retention, and sharing of a consumer's personal information to be "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed." The CPRA would also create a new consumer right that requires businesses to use commercially reasonable efforts to correct inaccurate personal information upon the request of a consumer (mirroring the right to rectification under the GDPR) and places new contractual and substantive obligations on service providers, similar to the distinct obligations the GDPR establishes for processors.

Furthermore, like the GDPR, the CPRA includes provisions that cover automated decision-making. The CPRA would require the Agency to issue regulations governing access and opt-out rights with respect to a business' use of automated decision-making technology, including requiring business to provide "meaningful information about the logic involved in such decision-making processes, as well as a description of the likely outcome of the process."

Creating Heightened Obligations for Certain Categories of Information. The CPRA would create a new category of "sensitive personal information" that requires distinct treatment. Sensitive personal information – which includes government-issued identifiers, account log-in credentials, financial account information, precise geolocation, contents of certain types of messages, genetic data, racial or ethnic origin, religious beliefs, biometrics, health data, and data concerning sex life or sexual orientation – would be subject to heightened notice requirements and a consumer's right to limit the processing of such data. The CPRA would also provide enhanced protection for the personal information of minors, clarifying that individuals under 16 must opt in for a business to sell "or share" their personal data.

Removing the Cure Period for AG Enforcement. The CPRA would remove the 30-day cure period for enforcement actions brought by the California Attorney General, while granting the Agency authority to provide a business a time period in which it may cure alleged violations. The law would retain the 30-day cure period for private claims related to data breaches, although the CPRA clarifies that "implementation and maintenance of reasonable security procedures and practices" does not constitute a cure with respect to such breaches.

Expanding the Private Right of Action. The CPRA would expand the private right of action in the CCPA – which presently applies only if there is a breach of a relatively short list of nonencrypted and nonredacted personal information – to apply to the unauthorized access or disclosure of an "email address in combination with a password or security question and answer that would permit access to an account" if the business failed to maintain reasonable security.

Changing the Definition of 'Business.' The CPRA would establish a higher threshold for the definition of "business." Under the CPRA, some small businesses that are currently required to comply with the CCPA would fall outside the scope of the CRPA, including those who share the personal information of fewer than 100,000 consumers.

If the CPRA passes in November, there will be over two years between adoption and implementation. The new California Privacy Protection Agency will assume rulemaking authority and would be required to adopt final regulations by July 1, 2022. As with the CCPA, there would be a six-month delay in enforcement after the CPRA goes into effect – the Agency would begin enforcement on July 1, 2023. In addition to giving businesses the opportunity to reassess their privacy compliance programs, the delayed implementation may also leave a window for the passage of a comprehensive federal privacy law that could potentially preempt the CPRA.

Beyond CPRA, California's Privacy Law Landscape Continues to Change

The ballot initiative that voters are considering follows on the heels of two enacted amendments to the CCPA. On September 29, California Governor Gavin Newsom signed AB 1281 into law, which extends the CCPA's exemption for employee and business-to-business personal information. Both exemptions were scheduled to sunset on January 1, 2021, but are now extended for at least an additional year (i.e., through January 1, 2022). Note, this extension will only take effect if the CPRA is *not* approved in November, as the CPRA would extend the business-to-business and employee exemptions through 2023. In either case, these exemptions will not sunset this January.

The Governor also signed AB 713, which amends the CCPA by explicitly exempting from the CCPA patient information that is de-identified, according to the HIPAA deidentification standard (rather than the CCPA deidentification standard). The amendment requires that starting January 1, 2021, any sale or license of such deidentified patient data must include specific contractual provisions that prohibit the purchaser or licensee from reidentifying the data or further disclosing the data to third parties who are not contractually bound by the same prohibition on reidentification.

Additionally, the California Attorney General's CCPA regulations continue to evolve. On October 12, 2020, the Attorney General's Office released the third set of proposed modifications to the CCPA regulations. This latest round of modifications proposed additions and deletions to the regulations that just became effective on August 14, 2020. Comments are due on the latest round of modifications by October 28, 2020.

***

It is more critical than ever that businesses keep their fingers on the pulse of emerging privacy laws in the United States. Our team has helped entities of all sizes from various sectors parse through complicated CCPA issues – from determining whether the CCPA applies to developing compliance programs. If your organization has questions about the CPRA or the possible impact of these developments, do not hesitate to reach out.