Stradling

California Voters Are Poised To Re-Write The CCPA Before Its First Anniversary

July 13, 2020

When California voters fill out their ballots this November, they'll have an opportunity to overhaul the country's most comprehensive consumer privacy law, which is barely six months old. The California Consumer Privacy Act (CCPA) took effect on January 1, 2020. On June 25, an initiative called the California Privacy Rights Act of 2020 (CPRA) officially qualified for the November ballot. The initiative, which is very likely to pass, would enact a package of significant amendments to the CCPA, adding, among other things, new consumer rights, the creation of a dedicated enforcement agency with the power to impose administrative fines, special rules for handling "sensitive" personal information, explicit restrictions on sharing personal information for purposes of interest-based advertising, and expanded liability for data breaches.

Why Is This Happening?

The CPRA ballot initiative was introduced by Californians for Consumer Privacy. That's the same non-profit organization behind the proposed 2018 ballot initiative that prompted the California Legislature to hastily enact the CCPA, which kept that initiative off the 2018 ballot. Following enactment, Californians for Consumer Privacy and other consumer advocacy groups expressed concern that the legislative process had diluted the CCPA. The CPRA, which some refer to as "CCPA 2.0," is, at least in part, an effort to enact even more robust consumer privacy protections that these groups originally envisioned.

Can We Expect Lawmakers To "Pre-Empt" This Ballot Initiative, Similar To What They Did By Passing The CCPA In 2018?

That looks unlikely. The Legislature has not given any indication that it will step in, and lawmakers may have less motivation to intervene this time around. If the voters enact the CPRA, the Legislature only needs a simple majority to amend it (so long as the amendment is consistent with and furthers the purpose of the initiative). That's different from the 2018 CCPA ballot initiative, which would have required a supermajority of the Legislature for any amendments.

What Are The Big Changes, And When Would They Take Effect?

The CPRA would take effect on January 1, 2023, and for most purposes would apply to personal information collected on or after January 1, 2022. There are several changes to expect. Here are eight of the most significant:

A Dedicated Enforcement Agency With Power To Impose Administrative Fines: Currently, the Attorney General is responsible for enforcing the CCPA. The Attorney General may file a civil action in court seeking monetary penalties and other relief for violations, but doesn't have the power to issue administrative fines. The CPRA would totally revamp enforcement by creating and funding the California Privacy Protection Agency, whose sole mission will be to enforce the CCPA. The agency would have subpoena and audit powers, and the power to impose administrative fines up to $7,500 per violation. It would also take over rule making from the Attorney General.

Mandatory Audits And Risk Assessments For "High Risk" Processing: The CPRA charges the new enforcement agency with issuing regulations requiring annual audits and periodic risk assessments by businesses that undertake high-risk processing of personal information. The final regulations, which presumably will include some guidance on what constitutes high risk processing, must be adopted by July 1, 2022.

Expanded Liability For Data Breaches: The CCPA already gives consumers a right to sue in the event of a breach of certain limited categories of sensitive personal information when the breach results from a business's failure to employ "reasonable security procedures and practices." Plaintiffs may sue on behalf of a class of consumers impacted by the breach and seek statutory damages of up to $750 per incident, per consumer, or actual damages, whichever is greater. The CPRA would broaden a business's exposure by adding "email address in combination with a password or security question and answer that would permit access to the account" to the categories of personal information that, if breached, would trigger the right to sue.

The Right To Request Data Correction: The CCPA created three key rights for California residents (consumers): the right to request access to their personal information, the right to request deletion of their personal information, and the right to request that a business stop selling their personal information (the right to "opt-out"). The CPRA would add the right to request correction of inaccurate personal information.

Restrictions On Use Of "Sensitive" Data: The CCPA didn't explicitly prohibit any particular uses of personal information. It only required that a business disclose, at or before the point of collection, the purposes for which data is used. Under the CPRA, consumers would have the right to restrict a business's use and disclosure of "sensitive personal information," defined as a subset of personal information, that includes social security number, driver's license number, passport number, financial account information and credentials, precise geolocation, racial or ethnic origin, religious or philosophical beliefs, union membership, the contents of personal communications, genetic data, biometric or health information, and information concerning sex life or sexual orientation. Business would be required to provide a mechanism by which a consumer could limit the business's use of their personal information to purposes necessary to perform a service or provide goods requested by the consumer.

The Right To Opt-Out Of "Sharing" Of Data For Interest-Based Advertising: One of the most difficult compliance challenges under the CCPA is its broad and vague definition of what constitutes a "sale" of personal information. A "sale" is defined to include, among other things, "making available, transferring, or otherwise communicating . . . a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration." This has generated an intense debate over whether the common practice of making personal information—such as IP address, device identifier, and browsing activity—available to ad networks or other third parties who deliver interest-based ads constitutes a "sale" in some or all circumstances.

The CPRA would resolve, or perhaps moot, at least some of this uncertainty by adding a new defined term—"share"—and placing explicit restrictions on "sharing" personal information. "Share" means sharing, disclosing, or otherwise making available to a third party a consumer's personal information "for cross-context behavioral advertising, whether or not for monetary or other valuable consideration." A consumer would have the right to direct a business to stop "sharing" their personal information, just as they already have the right to direct the business to stop "selling" it.

Explicit Data Minimization Obligation: The CCPA didn't directly restrict a business's ability to collect personal information. It merely required that businesses disclose the categories collected. But under the CPRA, a business's "collection, use, retention, and sharing" of personal information shall be explicitly limited to that which is "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 original context of collection.

New Rules For Automated Decision Making: The CPRA requires the Attorney General to issue regulations governing access and opt-out rights with respect to a business's "profiling," or automated decision making, based on personal information. "Profiling" includes "to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements," and will be further defined through regulation.

Takeaways

The CPRA would take California several steps closer to the European Union's model of data privacy regulation, embodied in the EU's General Data Protection Regulation (GDPR). The GDPR has required a right of correction, special restrictions for sensitive personal data, data minimization, and restrictions on automated decision making since it took effect in May 2018. But fundamental differences between the California and EU approaches would remain. For example, the GDPR prohibits any processing of personal information unless at least one of six "lawful bases" for processing applies. In practice, this means businesses must often get specific, opt-in consent simply to collect personal data that is governed by GDPR. The CPRA wouldn't go that far.

Nevertheless, the CPRA will pose unique compliance challenges to businesses between its likely enactment this November and January 1, 2023. There will be a roughly two-year period in which compliance programs must account for the CCPA of today (which continues to be plagued by a raft of ambiguities) while also anticipating the CCPA of tomorrow. The CPRA makes it all the more imperative that businesses gain a detailed and comprehensive understanding of their data needs, data flows, related risks, and the business impacts inherent in conforming products and services, operations, analytics, customer and vendor relationships, and online marketing efforts to existing and upcoming privacy requirements.

Authors:

Travis P. Brennan
949.725.4271
tbrennan@sycr.com

Mayant Luk
949.725.4057
mluk@sycr.com