CCPA 2.0 Gets Closer to Reality: CPRA Eligible for November 2020 Ballot; How Does it Compare to CCPA?

Alyssa Z. Hutnik

June 25, 2020

On June 24, 2020, the Secretary of State of California announced that the California Privacy Rights Act (CPRA), had enough votes to be eligible for the November 2020 general election ballot. CPRA is a ballot initiative, which, if adopted, would amend and augment the California Consumer Privacy Act (CCPA) to increase and clarify the privacy rights of California residents. The result is a law that is closer in scope to robust international privacy laws, such as the GDPR. For more information on the CCPA, please see our posts here.

To be eligible for the November 2020 ballot, CPRA needed to obtain over 623,212 verified signatures. If passed by a simple majority of California voters in November, as is looking likely, the CPRA will become effective on January 1, 2021, with most compliance obligations required by January 1, 2023. With the exception of the access right, the CPRA would apply only to personal information collected after January 1, 2022. Additionally, the CPRA would extend the CCPA's temporary business to business exemption and employee data exemptions (which are scheduled to sunset on January 1, 2021) until January 1, 2023.

Until January 1, 2023, businesses would need to comply with the CCPA and any finalized regulations in force (which could mean both CCPA and CPRA regulations). The Attorney General would preserve its authority to issue CCPA regulations and enforcement during this period, and a new privacy agency would be formed with its own rulemaking and enforcement authority.

For more information on the comparison between CCPA and CPRA, please see our chart below. While there are no immediate action items, companies may benefit from reviewing the CPRA requirements to assess what changes may be necessary should the ballot pass. And a reminder -- the CCPA enforcement date is set for July 1, 2020, although it is not yet clear whether the CCPA regulations will be effective by then; the Office of Administrative Law's review remains pending. Please contact any of the attorneys in Kelley Drye's Privacy Group if you would like assistance in California privacy compliance.

	CCPA	CPRA
“Business” Threshold	$25 million annual revenue; or 50,000+ consumers; or 50% of annual revenue derived from selling consumers personal data	$25 million annual revenue; or buys, sells or shares 100,000+ consumers or households; or 50% of annual revenue derived from selling or sharing consumers’ personal data
Operative date	January 1, 2020	January 1, 2023, and applies only to personal information collected on or after January 1, 2022, except with regard to access requests.
Employee and B2B exemptions	Sunsets January 1, 2021	Sunsets January 1, 2023
“Sold” and “Shared” Definitions	“Sell,” “selling,” “sale,” or “sold,” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating … for monetary or other valuable consideration.	The term “sold” is broadened to “sold or shared.” This change is accompanied by a change in the definition of what it means to sell, which removes the carve-out for sharing personal information with a service provider (although this point is addressed in a more narrow definition of “third party”).
Service Providers and Contractors	A Service Provider is an entity “that processes information on behalf of a business … provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business...”	Introduces new requirements to qualify as a “service provider” and adds a new definition of a “contractor” that mirrors the definition of a service provider. Clarifies and provides additional requirements regarding service providers’ use of the data, such as a requirement that service providers silo the data they learn about a consumer from other sources. (This is more restrictive than the AG CCPA regulations). Requires contractual terms, similar to the GDPR.
Consent	Consent is not required in the CCPA. However, the definition of sale contains guidance regarding “intentional interactions.”	Consent is defined as any freely given, specific, informed and unambiguous indication of the consumer's wishes by which he or she… signifies agreement to the processing of personal information relating to him or her for a narrowly defined particular purpose. Introduces the concept of “dark patterns” defined as a user interface designed or manipulated with the substantial effect of subverting or

		impairing user autonomy, decision-making or choice, as further defined by regulation. Agreement obtained through use of dark patterns does not constitute consent.
Sensitive information	Does not contain separate provisions for sensitive information (other than increased verification requirements.)	Contains disclosure, opt-out, and purpose limitation requirements for sensitive information.
Automated Decision-Making	N/A	Introduces concept of “profiling.” Calls for regulations requiring businesses' response to access requests to include meaningful information about the logic involved in such profiling, as well as a description of the likely outcome of the process with respect to the consumer.
Right to Correct	N/A	Gives consumers the right to correct inaccurate information.
Opt Out of Targeted Advertising	The CCPA does not restrict targeted advertising if it can be conducted without “selling” data.	Providing advertising or marketing services is a business purpose but this does not include “Cross-Context Behavioral Advertising,” a newly defined term to describe ads targeted to consumers based on a profile or predictions about the consumer related to the consumer’s activity over time and across multiple businesses or distinctly-branded services, websites or applications. Contains a broader opt-out provision (for both “sale” and “sharing”) and specifically limits service providers from engaging in any “cross-context behavioral advertising.”
Retention	The CCPA does not contain any requirements that businesses disclose their retention practices to consumers.	Businesses must disclose, at the time of collection: the length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine such period. A business cannot retain personal information for longer than is

		reasonably necessary for that disclosed purpose. Contains language to promote the following GDPR principles: • Data Minimization • Purpose Limitation • Duty to Avoid Secondary Use
GDPR Concepts .	N/A	
Enforcement	Enforced by the Attorney General Allows a 30 day period to cure violations	Establishes the California Privacy Protection Agency that would have a broad scope of responsibilities and enforcement powers. Security breaches include email/password/challenge questions. Modifies the 30-day cure period to apply to a private right of action for security breach violations, rather than for general privacy violations of the law. Fines for violations involving children's personal data are tripled.