Privacy Alert: 2020 Election Ushers in a New California Privacy Rights Act (aka “CCPA 2.0”)

November 4, 2020

Compliance with the California Consumer Privacy Act (the "CCPA"), a first of its kind commercial privacy law, has been a top business priority since June 2018. With the ink barely dry on the California Attorney General's latest set of CCPA regulations, California voters have overwhelmingly approved another data privacy law, the California Privacy Rights and Enforcement Act of 2020 (the "CPRA"). The CPRA narrows the CCPA's definition of a "business," but adds new requirements and expands consumer rights at the same time. Although the new Act does not go into effect until January 1, 2023, it will have a "look back" to January 2022. Businesses need to start addressing their CPRA compliance issues now.

The CPRA reduces the scope of the CCPA by increasing the threshold number of California residents and households reached from 50,000 to 100,000, and eliminating the number of devices as a factor. Privacy advocates argued this higher threshold was a step backwards, but businesses will appreciate the modification. The CPRA also clarifies that the annual gross revenue threshold of $25 million is to be determined each January 1, based on the preceding year's revenue. The CPRA also amends definitions of "service provider," "third party," and "contractor" so as to increase the scrutiny of a business' contractual obligations with these entities.

The CPRA enhances the CCPA's consumer privacy rights, which included the rights to access, delete and opt out of the sale of personal information. The new Act provides consumers the right to correct inaccurate personal information and to opt out of sharing (as opposed to selling) it with third parties. The CPRA also creates a new category of "sensitive personal information," which includes geolocation and biometric data, certain financial information, race, ethnic origin and other data points. Consumers will have the right to limit a business' use and disclosure of this sensitive information except as necessary to perform the services or provide goods reasonably expected by the consumer.

The CPRA creates a new "California Privacy Protection Agency" that will administer, implement, and enforce the CPRA, after pro-consumer groups complained that the CCPA enforcement was understaffed and underfunded by the California Attorney General's Office. The law mandates approximately $10 million in funding for this new privacy agency, and authorizes it to levy fines of up to $7,500 for statutory privacy violations. The CPRA eliminates the CCPA's 30-day cure period to remedy defects in compliance, increasing

compliance risks to businesses.

The CPRA includes other modifications and new requirements, and the Lathrop GPM team is prepared to guide businesses through the increasingly complex data privacy regime. For example, the CPRA extends the CCPA's moratorium on employee data, which makes employee data exempt from the acts, until January 1, 2023. In the meantime, additional legislative efforts, whether to amend the CPRA or as a stand-alone bill, addressing employee data and rights are likely to be presented during future legislative sessions.

Under the CCPA and CPRA, California currently sets the standard for data privacy in the United States. To comply, businesses must evaluate data systems and security protections, ensure privacy notices and practices are sufficient, and update and inventory third-party and vendor agreements. If you have any questions regarding the CCPA or the new CPRA, please contact the Lathrop GPM Privacy Team.