Expansive New California Privacy Measure Cleared for November Ballot

June 25, 2020

While businesses operating in California are still adjusting to the requirements of the California Consumer Privacy Act (CCPA) and are watching for enforcement actions brought by the California Attorney General, as its enforcement powers begin on July 1, an expansive new privacy initiative was certified today by the California Secretary of State to appear on California ballots in the November election.

Today, the California Secretary of State certified that the California Privacy Rights Act (CPRA) had obtained sufficient signatures to qualify as a ballot initiative in California's November 2020 election. The CPRA is intended to replace the CCPA, dramatically expanding privacy protections for consumers and liabilities for businesses subject to the law, including in several ways discussed below.

While the CPRA would not go into effect until January 1, 2023, businesses will want to keep a close watch on developments in order to have as much time as possible to prepare if the measure is approved. The majority of the CPRA's provisions would apply to personal information collected on or after January 1, 2022 (personal information collected in the context of employment and business-to-business communications would initially be excluded, as in the CCPA) and experiences with the General Data Protection Regulation (GDPR) and CCPA reinforce the importance of early compliance efforts. Even several years' advance notice of the enforcement of privacy laws, such as with the GDPR in the European Union and the CCPA, has challenged the capacity for businesses to build adequate compliance programs. Fortunately, several of the provisions of the CPRA bring California law much closer to the requirements of the GDPR, a boon, but not a panacea, for businesses that are already compliant with that law.

There has been little polling for the initiative, but at least one **survey** of Californians shows strong support for expanded privacy legislation. California saw a similarly supported privacy-focused ballot initiative in 2017, which the California House and Senate obviated by unanimously passing the CCPA. Whether the CPRA initiative succeeds this fall or spurs the legislature to proactively enact similar protections, companies that do business in California should stay tuned to the fate of the initiative and be mindful of its potential impact on their operations.

Highlights of the CPRA

- *New protections for "sensitive personal information."* The CPRA would create a category of sensitive personal information—such as government identifiers, precise geolocation information, and financial, racial, and genetic data—which would be subject to additional protections, including additional notice at collection, as well as consumers' rights. Notably, the CPRA, unlike the GDPR, would not require express (explicit) consent for collection of sensitive personal information. The scope of sensitive personal information would differ from "special categories of personal data" under the GDPR, so businesses may need to revisit data management structures to ensure they are able to comply with obligations regarding the new category of sensitive personal information.
- *Right of correction.* The CPRA would require businesses to use commercially reasonable efforts to correct inaccurate personal information if requested through a verifiable consumer request. As businesses review their practices to respond to consumer requests under the CCPA, businesses would be well suited to begin to assess whether their infrastructure also will allow for correction of personal information records. A right of correction already exists

under the GDPR, so businesses covered by the GDPR should consider whether they already have sufficient mechanisms in place to allow for the new right of correction under the CPRA.

- *Evolving enforcement provisions.* The CPRA would include a number of provisions that could potentially expand covered businesses' liability, both from actions brought by private plaintiffs and from California regulators. The CPRA identifies an additional group of consumers not included in the CCPA who would be able to bring a private right of action: those whose email addresses, together with either the password or security question answer, are subject to unauthorized access and exfiltration, theft or disclosure as a result of the business's violation of its duty to implement and maintain reasonable security procedures and practices. Additionally, the CPRA would increase penalties for any violation of the CPRA with respect to personal information for consumers whom the business knows to be under 16 years of age. Such businesses could be fined $7,500 for any violation of the CPRA with respect to such personal information without a finding of intent. The CPRA would also establish a new regulatory body, the California Privacy Protection Agency, which would be responsible for enforcing the CPRA. However, the CPRA does not preclude the California Attorney General from enforcing other relevant California laws regarding data security and unfair and deceptive acts, so a data security incident could potentially give rise to multiple California regulatory investigations. Given the increased possibility of private actions and liability, businesses may want to review existing security and storage procedures, including with respect to minors' personal information.
- *Restrictions on "sharing" of personal information.* While the CCPA currently provides for obligations and rights tied to the sale of personal information, obligations and rights under the CPRA would apply to both the sale and the "sharing" of personal information, which would include renting, releasing, disclosing, making available or otherwise communicating a consumer's personal information to a third party for cross-context behavioral advertising, regardless of the consideration provided. This revision would clarify that the requirements of the CPRA, including a consumer's right to opt out, unequivocally applies to behavioral advertising.
- *Additional security and risk assessment requirements.* The CPRA would require all covered businesses to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect personal information from unauthorized or illegal access, destruction, use, modification or disclosure, as well as limit the collection and use of personal information to what is reasonably necessary to achieve the businesses' specified purposes. Both of these changes apply new obligations on businesses not present in the CCPA. Additionally, any business whose processing of personal information presents "significant risk to consumers' privacy or security" (based on the size and complexity of the business and nature and scope of the processing activities) would be required to perform annual cybersecurity audits and regularly submit risk assessments to the new California Privacy Protection Agency regarding the processing performed by the business and how the business has weighed the benefits of that processing for the business, consumers, the public, and other stakeholders against consumers' privacy rights.
- *Requirements on third parties.* The CPRA would require that businesses that share, sell or disclose personal information to a third party, service provider or contractor contractually obligate these counterparties to comply with the CPRA. Additionally, any such third party, service provider or contractor would be required to cooperate with the business in responding to a consumer's verifiable requests, including to correct, delete or limit the use of certain personal information. This would broaden third parties' obligations beyond what currently exist under the CCPA—bringing California law closer to the requirements of the NY Stop Hacks and Improve Electronic Data Security ("SHIELD") Act, the NY Department of Financial

Services Cybersecurity Regulation and the GDPR, among other privacy regimes—and businesses would need to reassess their contracts with such third parties to ensure that those agreements comply with the CPRA.

- *Regulation of automated decision making.* The CPRA would require the California Attorney General to issue regulations governing consumers' rights to access information about, and opt-out of, automated decision making technology, including any automated processing of personal information to evaluate a person or predict a person's economic situation, health, personal preferences or behavior, among other forms of profiling. Businesses that build profiling into products and services should be prepared to provide additional disclosures or modify these practices. This change would be analogous to certain provisions of the GDPR, which provide data subjects with the right to not be subject to automated decision making.

For analysis of the CCPA and what businesses can do to comply with existing California requirements, please see our previous client memoranda and blog posts, available **here**, **here** and **here**.

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

Frank J. Azzopardi	212 450 6277	**frank.azzopardi@davispolk.com**
Robert A. Cohen*	202 962 7047	**robert.cohen@davispolk.com**
Pritesh P. Shah	212 450 4147	**pritesh.shah@davispolk.com**
Matthew J. Bacal	212 450 4790	**matthew.bacal@davispolk.com**
Daniel F. Forester	212 450 3072	**daniel.forester@davispolk.com**
Matthew A. Kelly	212 450 4903	**matthew.kelly@davispolk.com**
Will Schildknecht	212 450 3557	**will.schildknecht@davispolk.com**
Jennifer Leather	650 752 2077	**jennifer.leather@davispolk.com**

* Mr. Cohen is admitted to practice in New York and Maryland, and is practicing in DC under supervision of partners of the firm.