PRIVACY & DATA SECURITY ALERT | NOVEMBER, 2020

California Votes To Strengthen Consumer Privacy Laws

By Stephenie Wingyuen Yeung

On November 3, 2020, Californians voted to approve Proposition 24 to strengthen the California Consumer Privacy Act ("CCPA"). Any company that does business in California and that is subject to the CCPA will now have to spend the next few years preparing to comply with what has been called "version 2" of the CCPA.

Passage of Proposition 24, the Consumer Privacy Rights and Enforcement Act of 2020 ("CPRA" or the "Act"), comes only four months after CCPA became enforceable, and only twelve weeks after the California Attorney General's Office published the final implementing regulations of the CCPA. Proponents of the ballot initiative hope that the CPRA will refine current CCPA provisions and expand consumer rights over business collection, use, sale or sharing of their personal information.

WHEN WILL THE CPRA COME INTO EFFECT?

In California, initiative measures generally take effect 30 days after the certification of the vote. Measures may also provide a different operative date.

Five provisions of CPRA will become effective five days after the November 3 vote is certified:

- A Consumer Privacy Fund will be established;
- A new state enforcement agency, the California Privacy Protection Agency ("CPPA"), will be created;
- The California Attorney General will be directed to adopt implementing regulations for the CPRA and the mechanism to transfer regulatory authority to the CPPA;
- Designate funds for the CPPA; and
- The current operative dates concerning employee data and B2B data will be further extended to January 1, 2023.

The remaining provisions of the CPRA will become operative on January 1, 2023, with a look-back period for the consumer right of access of at least 12 months.

WHAT'S NEW IN THE CPRA?

Many of the details of the CPRA will be clarified in the implementing regulations. Below is an overview of some of the most significant provisions.

The Act contains some business-friendly revisions to the CCPA:

- Changes the threshold quantity of annual processing of the information of 100,000 consumers or households, thereby exempting smaller businesses from CCPA compliance.
- Allows businesses to call data sharing arrangements that are not actual sales to be called "sharing" arrangements instead of "sales" in notices to consumers.
- Creates a new designation of "contractors" – persons to whom a business discloses or makes available personal information for a business purpose pursuant to a contract – that, like service providers, would not be responsible for responding to consumer rights requests, but must assist businesses in complying with the response.
- Expands the definition of "publicly available" data to include public profiles and information that a business has a reasonable basis to believe are lawfully made available by the consumer. For example, a California resident's Twitter or LinkedIn profile

would not be considered sensitive personal information.

- Explicitly excludes trade secrets from the Act.
- Relieves a business from having to provide individualized responses to verified consumer rights requests if the responses are identical to what is in the business's privacy policy.
- Relieves a business from responding to requests for deletion and access requests for many types of unstructured data.
- Requires a business to provide notice about the collection, use, or sale of children's personal data only if the business has actual knowledge that it is collecting such data from children under the age of 16.

The CPRA imposes an affirmative requirement on businesses to implement **reasonable security procedures and practices** to protect consumer personal information. The same level of privacy protection must be required of the business's service providers, contractors, and third parties.

The Act designates a **new category of Sensitive Personal Information**, which includes personal information that reveals:

- A consumer's social security, driver's license, state identification card, or passport number;
- A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
- A consumer's precise geolocation;
- A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
- The contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication;
- A consumer's genetic data, and the processing of biometric information for the purpose of uniquely identifying a consumer;
- Information about a consumer's health; or
- Information about a consumer's sex life or sexual orientation.

Businesses will have **additional notice obligations**. They must inform consumers of the collection, processing, and disclosure of sensitive personal information, if the personal information will be sold or shared, and how long each category of personal information will be retained. These notices must be provided at or before the point of collection.

Consumers will have **additional privacy rights**, including the right to limit a business's ability to use sensitive personal information. Other new consumer rights under CPRA include the right to correct inaccurate personal information and the right to request access to how and with whom a business shared or sold any personal information beyond a twelve month period.

The CPRA seeks to **tighten the Adtech industry's use of personal data** by closing what has been perceived as a loophole in the CCPA. While the CCPA's "Do Not Sell" and opt-out provisions were intended to give consumers broad control over how companies share and disclose their data, some companies have argued that those provisions do not apply to their sharing of data with target advertising platforms because money isn't exchanged for data. Instead, the target advertising platforms are the companies' service providers and no "sale" of the personal information occurs. The CPRA closes this gap by expressly including cross-context targeted advertising transactions in the definition of sharing and giving consumers the right to control the sharing of their personal information.

Additional contractual requirements will be imposed on service providers, contractors, and third parties. These include:

- Specify that the information disclosed or sold by the business is only for limited and specified purposes;
- Require the service provider, contractor, or third party to comply with the CPRA and to provide the same level of privacy protection as mandated by the Act;
- Require the service provider, contractor, or third party to notify the business if it can no longer do so;
- Obligate the service provider, contractor, or third party to only use personal information in a manner

consistent with the business's obligations under the CPRA; and

- Allow the business to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

Agreements with contractors must also prohibit the contractor from selling or sharing the personal information it receives or using or disclosing the personal information for any purpose other than those specified in the agreement. In addition, agreements should prohibit the contractor from aggregating the personal information with other data received or collected through other means.

In cases of **high risk processing**, the CPRA will require annual audits and risk assessments that will be prescribed through the implementing regulations.

Where the processing involves **automated decision making or profiling**, the Act creates new access and opt-out rights that will also be clarified in the implementing regulations.

The Act significantly strengthens enforcement by creating a **new state enforcement agency** – the California Privacy Protection Agency ("CPPA" or the "Agency") – that will be established in 2021. The Agency will be vested with the full administrative power, authority, and jurisdiction to implement the CCPA and will take over the enforcement of the CCPA and eventually the CPRA from the Office of the Attorney General. The Agency will also be responsible for making grants to non-profit organizations to promote and protect consumer privacy, to educate children about online privacy, or to fund cooperative programs between state and local law enforcement and international law enforcement organizations to combat fraudulent activities with respect to consumer data breaches.

Currently, CCPA allows a business that has been notified by the Attorney General of an alleged violation to cure it within a thirty-day period to avoid administrative fines. The CPRA strengthens enforcement by **eliminating the opportunity for businesses to cure** alleged violations in an administrative enforcement action. The Act also limits a business's defense to private actions, mandating that the implementation and maintenance of reasonable security procedures and practices following a breach does not constitute a cure with respect to that breach.

Fines for violations of the Act involving children's personal information will be increased to $7,500 per violation.

WHAT SHOULD COMPANIES DO NOW?

Companies subject to CCPA should assess whether the increase in the data processing threshold changes their obligations to comply with the CPRA.

Companies that will continue to be subject to the CPRA should take advantage of their recent compliance efforts and review the current security and privacy policies and procedures as well as their compliance programs to identify any changes that are necessitated by the new requirements. Over the next year, companies should monitor the rulemaking efforts to further identify, plan for, and incorporate any new obligations.

Companies should also review their contractual relationships with service providers, contractors, and other third parties to layer new requirements into those service agreements. ◆

For more information about Schnader's Privacy and Data Security Practice Group or to speak with a member of the firm, please contact:

Stephenie Wingyuen Yeung
Co-Chair, Privacy and Data Security Practice Group
215-751-2277
syeung@schnader.com

Anne E. Kane
Co-Chair, Privacy and Data Security Practice Group
215-751-2397
akane@schnader.com