GT GreenbergTraurig

Alert | Data, Privacy & Cybersecurity

January 2020

‘CCPA 2.0’ Ballot Initiative Could Result in Big Updates to California Privacy Law

Although the California Consumer Privacy Act (CCPA) has only been in effect for a matter of weeks – and its proposed regulations are not yet finalized – it could be overhauled by a new privacy law later this year.

Last fall, the group that first formulated the CCPA as a ballot initiative in 2018, Californians for Consumer Privacy, led by real estate developer-turned-privacy activist Alastair Mactaggart, timely submitted a ballot measure and subsequent amendments, now titled “The California Privacy Rights Act of 2020” (CalPRA or “the Act”). The group is likely seeking to utilize a ballot initiative for this legislative update to avoid the lobbying and amendment process it believes could compromise the rights and obligations that the initiative sets forth. To guard against later amendments that limit the law’s application, the Act permits amendments by majority vote in each house of the California Legislature and signed by the governor; however, such amendments must be “consistent with and further the purpose and intent of this Act as set forth in Section 3.” In all likelihood, this last provision is one that will be contested in the future.

While retaining many CCPA provisions, CalPRA proposes significant updates to the CCPA, and seeks for the CA attorney general’s office and a newly formed privacy agency to issue guidance and regulations on various issues. If passed, the Act would require impacted organizations to make further changes to their data protection practices. However, unlike the CCPA, under CalPRA, California may provide organizations with some guidance on how to comply with CalPRA prior to the operative date of the new law.

Deadlines

For CalPRA to appear on the November 3, 2020, general election ballot, it must receive 623,212 signatures, according to the California Secretary of State's website. Given the public awareness raised by the CCPA, the signature threshold requirement will likely be met by the June 25 deadline. If CalPRA is on the voting ballot, passage of a ballot measure providing consumers with more rights seems probable, especially given that it is a U.S. presidential election year with high voter turnout expected.

Effective Dates

The ballot initiative sets January 1, 2023, as the operative date (applying to personal information collected on or after January 1, 2022), and until then the CCPA will remain in "full force and effect." However, the Act identifies a few CalPRA provisions as having an effective date of January 1, 2021.

- **Employee and Business-to-Business Exemptions**. As amended by the governor in October 2019, the CCPA contains exemptions for employee and contractor personal information and personal information exchanged in B2B communications. These exemptions are set to expire on January 1, 2021, but the Act would extend these exemptions to January 1, 2023.
- **Rulemakings**. CalPRA requires the state attorney general to initiate rulemakings covering more than 20 wide-ranging topics involving definitions, exemptions, technical specifications for opt-out preference signals, automated decision-making, cybersecurity audits and risk assessments, and adjusting monetary thresholds for "business" eligibility. The effective date of these rulemaking provisions would be January 1, 2021, to ensure guidance is provided before CalPRA becomes fully operative in 2023.
- **CPPA**. CalPRA establishes a California Privacy Protection Agency (CPPA) within the state government, vested with full administrative power, authority, and jurisdiction to implement and enforce the privacy law. The effective date for establishment of the CPPA is January 1, 2021, presumably to ensure the governing body's ability to enforce the new privacy law is fully active by January 1, 2023, when the Act takes full effect.

Sensitive Personal Information Defined

In contrast to the CCPA, CalPRA refers to and defines "sensitive personal information" (SPI). It does so in what amounts to an amalgam of elements from the GDPR's "special categories of personal data" definition (e.g., pertaining to race/ethnicity, religion, sex life, biometrics, or health) and additional elements. SPI includes personal information that reveals the contents of a consumer's mail, email, and text messages; a consumer's account log-in, debit card, or credit card number in combination with any password or access credential; or a consumer's "**precise geolocation**" (a newly defined term meaning any data derived from a device intended to be used to locate an individual within a 1,850-foot radius).

- **Consumer Notice**. Businesses controlling SPI collection must inform consumers, at or before the point of collection, as to the categories of SPI and purposes of its collection; whether such SPI is sold or shared; and the intended retention period for each category of SPI.
- **Right to Limit SPI Use**. Consumers retain the right to limit a business's use of SPI – and that of its service providers and newly defined "**contractors**" – to only that which is necessary to perform the services or provide the goods "reasonably expected by an average consumer."

- **Website Link(s)**. The Act retains the CCPA's requirement that a business that sells or shares consumers' personal information or uses or discloses consumers' PI other than as necessary or as reasonably expected (as noted immediately above) must provide a conspicuous "Do Not Sell or Share My Personal Information" link on its Internet homepage, enabling opt-out of the sale or sharing of such PI. However, under CalPRA, such businesses must provide a separate link titled "**Limit the Use of My Sensitive Personal Information**," enabling consumers to limit the use or disclosure of their SPI. The Act does permit a single link if it takes the consumer to a webpage allowing both opt-out of the sale of PI and limitation of SPI use.

Enforcement Procedures Changed

The Act does away with the CCPA's allowance in Section 1798.155(b) that "a business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance." CalPRA instead appears to reserve a 30-day cure period only as a means of preventing individual or class-wide statutory damages as part of a private right of action for security breach violations, rather than for general violations of the law.

The newly established privacy agency, the CPPA, will have the authority to investigate possible violations of CalPRA brought to its attention by any person's sworn complaint or its own initiative. The CPPA will provide the alleged violator notice of the alleged violation, and a summary of the evidence. The alleged violator will have at least 30 days from receiving such notice to appear, with its counsel, before the CPPA in a private proceeding and explain why probable cause to believe CalPRA has been violated does not exist. If the CPPA determines probable cause exists for believing CalPRA was violated, a hearing will be conducted in accordance with the Administrative Procedure Act, and will be overseen by an administrative law judge. If the CPPA finds that a violation of CalPRA has occurred, it can order the violating party to pay an administrative fine of up to $2,500 for each violation, or up to $7,500 for each intentional violation and each violation involving children's personal information.

Children's Personal Information

CalPRA triples the administrative enforcement fines to $7,500 per intentional violation for any business, service provider, contractor, or other person that violates the Act's requirements with respect to the collection or sale of the personal information of minors under the age of 16 without consent.

Cross-Context Behavioral Advertising

One of the goals of the Act appears to be to clarify the narrow role of newly defined "cross-context behavioral advertising" (CCBA).

- **CCBA Definition**. The Act effectively (albeit somewhat unclearly) describes CCBA as a business's targeting of advertising to a consumer based on PI about the consumer obtained from his or her interactions on websites, mobile applications, or services where the consumer is not currently directly engaging (i.e., non-first party).
- **Sharing**. Moreover, throughout CalPRA reference is made to "selling or sharing," with the latter term defined as disclosing, making available, transferring, or otherwise communicating a consumer's personal information "by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration."
- **Business Purpose**. The Act's definition of "business purpose," for which service providers or contractors may use a consumer's personal information for certain operational purposes and not have

it be treated as a "sale" to a "third party" (provided certain written contractual limitations on further retention, use or disclosure are in place), includes a revised subsection for "providing advertising and marketing services, except for cross-context behavioral advertising…"

Taken as a whole, CalPRA takes a highly restrictive stance with respect to traditional data-driven advertising and marketing, effectively treating as a likely sale any activities beyond first-party contextual advertising and non-personalized advertising not based on a profile or predictions derived from a consumer's inferred, past online interactions. It remains to be seen how the current industry-led CCPA "Do Not Sell" compliance regimes will be forced to evolve as a result of these renewed definitions, which attempt to paint a more unequivocal picture with respect to the sale classification of traditional third-party interest-based advertising.

Additional Important CalPRA Provisions

The Act proposes a number of other updates to the CCPA:

- **Business Definition**. The Act doubles from 50,000 to 100,000 one of the CCPA's "business" eligibility thresholds for an entity that "alone or in combination, buys or sells or shares the [personal information] of 100,000 or more consumers or households." It also removes from that criteria the business's need for a "commercial purpose" in its buying or selling of personal information, and, curiously, removes "devices" from the list with "consumers or households." CalPRA adds to the definition of "business" joint ventures or partnerships composed of businesses in which each business has at least a 40 percent interest (with each business composing the joint venture or partnership being separately considered a single business).
- **Publicly Available Information**. The "publicly available information" exclusion from the CCPA's definition of "personal information" is expanded under the Act to include information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer from widely distributed media. It also includes "information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience." This seems to suggest that the content of social media postings made without restrictions as to who may view the post will not be treated as personal information under CalPRA.
- **Correction**. Fixing a glaring omission in the CCPA, the Act provides consumers the right to correct inaccurate personal information held about them by a business, and requires businesses to inform consumers of this right.
- **Trade Secrets Exemption**. CalPRA clarifies that a business is exempt from disclosing information in response to rights requests, or in relation to cybersecurity audits or risk assessments, that would disclose the business's trade secrets.
- **Contractors and Contractual Flow Down**. The Act introduces "contractors" as persons to whom a business makes available a consumer's personal information for a business purpose pursuant to a written contract, as is also the case with service providers – i.e., persons who process personal information "on behalf of" a business. Under the Act, a contractor or service provider must notify the business if it wishes to engage any subprocessors, and it must do so "pursuant to a written contract binding the other person to observe all the requirements" of the underlying written contract it has with the business.
- **Retention Periods**. In a departure from the CCPA, the Act requires that consumers be notified of the length of time a business intends to retain each category of personal information or SPI, and that such information may not be held "for longer than is reasonably necessary for that disclosed purpose."

- **Possible Risk Assessments**. Whereas an earlier version of the ballot initiative called for the AG to issue regulations requiring "large data processors" – a term removed from the current version of the text – to perform annual cybersecurity audits and risk assessments that balance the risks and benefits of PI processing, the final version of the Act requires the AG to issue regulations on such annual cybersecurity audits and risk assessments for "businesses whose processing of consumers' [PI] presents significant risk to consumers' privacy or security."

***

Follow additional updates on the Data Privacy Dish blog, or reach out to the Greenberg Traurig Data, Privacy & Cybersecurity team for more information about the CCPA or the CalPRA ballot initiative's specific applicability to your organization.

Authors

This GT Alert was prepared by **Gretchen A. Ramos** and **Darren Abernethy**. Questions about this information can be directed to:

- Gretchen A. Ramos | +1 415.655.1319 | ramosg@gtlaw.com
- Darren Abernethy | +1 415.655.1261 | abernethyd@gtlaw.com
- Or your Greenberg Traurig attorney