DAVIS GILBERT

And the Winner of This Year's Election Is… the California Privacy Rights Act

The Bottom Line

- *Now that California voters have approved the CPRA, also known as "CCPA 2.0", businesses should review (or create) their privacy programs to ensure compliance with the CCPA (in its current form, including the recently finalized regulations) as well the new changes that will take effect under the CPRA.*

While the 2020 United States presidential election took center stage, California voters approved the California Privacy Rights Act (CPRA) ballot measure. The CPRA makes significant changes to the existing California Consumer Privacy Act (CCPA), the landmark state privacy law that went into effect on January 1, 2020. This means that many businesses will have to revisit their CCPA compliance programs (again). For those who have yet to develop a privacy compliance program, now is an opportune time to put one in place while considering the new changes that are on the horizon.

Although most of the CPRA becomes operative on January 1, 2023, it's important to understand that the CPRA will apply to personal information collected by a business starting on January 1, 2022. While the industry has lobbied hard to amend the CCPA, the CPRA will be much harder to revise since it is a ballot initiative passed by the voters. In addition, there are a handful of provisions that will become effective five days after the California Secretary of State has certified the election results, which is expected in early December. Notable among these changes are:

- An extension of the CCPA's temporary exemptions that apply to certain business-to-business (B2B) and employment related personal information until January 1, 2023. This overrides a shorter extension that passed earlier this year, as discussed in our recent alert;
- The establishment of $10 million in funding for the "California Privacy Protection Agency," a new agency that will have full authority to implement and enforce the CCPA, and will be responsible for adopting new regulations pursuant to the CPRA. The new agency will be governed by a five-member board that must be appointed within 90 days of the effective date of the CPRA; and
- Substantially expanded instructions to the Attorney General and the California Privacy Protection Agency to adopt new regulations. The new agency will be required to begin rulemaking activity as of the later of July 1, 2021 or six months after the new agency provides notice to the Attorney General that it is prepared to do so.

In addition, businesses should take a closer look at key CPRA changes that will become effective in the (not so distant) future. Keep in mind that the CCPA already requires updates to a privacy policy every 12 months.

- **"Business" Thresholds**: The key threshold that triggered the CCPA for many companies was the purchase, receipt, sale or sharing of the personal information of 50,000 or more consumers, households or devices. For many, just the existence of a website was enough to meet this threshold given the expansive definition of personal information included data elements such as cookie IDs, IP address and

device identifiers. The CPRA modifies this threshold by limiting its application to the purchase, sale or sharing (but not the receipt) of personal information of 100,000 or more consumers or households (excluding devices).

- **Sensitive Personal Information**: The CPRA adds a new definition for "sensitive personal information" which is a subset of personal information and includes government identifiers; account and login information; precise geolocation data; race; ethnicity; religion; genetic data; union membership; contents of private communications; and information concerning a consumer's sex life, sexual orientation, health and biometric information. Businesses who collect or process sensitive personal information, which specifically includes precise location data, will have to comply with new transparency requirements and offer consumers the ability to limit the use and disclosure of such data through a new link on the business' webpage, titled "*Limit the Use of My Sensitive Personal Information*".

- **Cross-Context Behavioral Advertising**: The CPRA amends the CCPA to explicitly address "cross-context behavioral advertising" which is defined as "the targeting of advertising to a consumer based on the consumer's personal Information obtained from the consumer's activity across businesses, distinctly-branded websites, applications or services, other than the business, distinctly-branded website, application or service with which the consumer intentionally Interacts." Significantly, the CPRA treats the "sharing" of any personal information for the purpose of cross-context behavioral advertising in the same way as a "sale" of personal information under the CCPA. Among other things, this means that businesses will need to make specific disclosures and offer certain rights with respect to personal information that has been "shared" for cross-context behavioral advertising. For example, this includes the right to opt out of such sharing through a link available on the business' webpage, titled "*Do Not Sell or Share My Personal Information*."

- **Advertising and Marketing**: The CPRA introduces a new "business purpose" which allows service providers and contractors to process personal information to provide "advertising and marketing" services, but specifically excludes use for cross-context behavioral advertising (discussed above). This appears to prevent any entity processing personal information for cross-context behavioral advertising purposes from being a "service provider" or "contractor" and the disclosure of personal information for such purposes will be subject to the opt-out rights discussed above. Taken together, the introduction of the "cross-context behavioral advertising" and "advertising and marketing" concepts appear to be an attempt to ensure that businesses must offer California residents the right to opt-out of cross-context behavioral advertising, regardless of any industry attempts to limit the application of such rights.

- **Publicly Available Information**: The carve-out of "publicly available" information from the definition of personal information was narrowly defined under the CCPA and only included information lawfully made available from government records. The CPRA expands this carve out to include information that a business reasonably believes is lawfully made available to the general public by the consumer or from widely distributed media. Ostensibly, this would appear to provide considerable relief for companies that primarily process personal information that has been publicly posted by the consumer through social media and similar channels.

- **Right to Correction**: In addition to the consumer rights discussed above (in relation to sensitive personal information and cross-context behavioral advertising), the CPRA also establishes a new consumer right to correct inaccurate personal information in a manner similar to that set forth in the EU's General Data Protection Regulation (GDPR).

- **General Duties**: In a nod towards Europe's GDPR processing principles, the CPRA introduces certain key "general duties" that apply to businesses. These include, among other things, an obligation to use reasonable security procedures and practices to protect personal information, restrictions against using

personal information for new purposes that are incompatible with the specified purpose for which it was collected and limitations on the retention of personal information for longer than is reasonably necessary for a disclosed purpose.

- **Contracts**: While the CCPA incentivized businesses to enter into certain agreements when sharing personal information, the CPRA now explicitly requires such agreements. Certain provisions are required to be included in these agreements and are clearly aimed at ensuring that the business has obtained assurances that the personal information will be adequately protected. Similarly, service providers and contractors are required to flow down certain mandatory provisions to any persons that they engage (or that those persons may engage) to assist with the processing of personal information on behalf of the business.
- **Increased Fines / No Cure Period**: Under the CPRA, the $7,500 maximum fine for a privacy violation will also apply to violations involving the personal information of minors under 16. Currently, only intentional violations are subject to the maximum fine. All other violations will remain subject to a fine of up to $2,500 for each violation. The CCPA's 30 day cure period for violations has also been eliminated.
- **Private Right of Action**: Although the CPRA largely retains the limited private right of action that consumers can bring in connection with a security breach, the scope of the private right of action has been expanded to include breaches exposing a consumer's email address in combination with a password or security question and answer that would permit access to the account.

Related People

Richard S. Eisert
Partner/Co-Chair Advertising + Marketing
212 468 4863
reisert@dglaw.com

Gary Kibel
Partner
212 468 4918
gkibel@dglaw.com