McELROY, DEUTSCH, MULVANEY & CARPENTER LLP

MDM&C Update

Click Here to Learn More About MDM&C >

November 10, 2020

CALIFORNIA PASSES PRIVACY LAW BALLOT INITIATIVE

In the November 3rd General Election, California voters resoundingly approved Proposition 24, a ballot initiative launched by privacy activist and real estate tycoon Alistair McTaggart to superimpose his proposed information privacy measure over the California Consumer Privacy Act (CCPA), the comprehensive California information privacy statute enacted in 2018 that took effect on January 1, 2020. If Proposition 24, which known as the California Privacy Rights Act (CPRA), becomes law, it is slated to take effect on January 1, 2023. California would then have a consumer privacy law more closely aligned with the European Union General Data Protection Regulation (GDPR) than any other state in the U.S.

Motivations for Replacing the CCPA by the CPRA

McTaggart indicated to reporters and the International Association of Privacy Professionals (IAPP) that he resorted to a ballot initiative as an almost amendment-proof legislative vehicle to protect the privacy protections enshrined in the CCPA, which McTaggart also spearheaded, from industry attempts to water down consumer protections. Moreover, CPRA proponents, like many others, realized that the CCPA fell short of achieving a meaningful level of consumer protection in a number of areas.

The CCPA in a Nutshell

The CCPA is, in essence, a "notice & access" statute using a broad EU-style comprehensive concept of "Personal Information." By contrast, most U.S. privacy laws protect only a limited number of data categories.

While the CCPA only provides rights to California residents ("consumers" in the CCPA's diction), its jurisdictional reach extends in principle to business operating and located outside California that are deemed to be doing business in California and meet certain thresholds.

In principle, the CCPA does not restrict the legal ability of covered businesses to collect, process, analyze and share personal information as long as the existence and purpose of those types of operations is properly disclosed to a consumer. A limited restriction on the use of personal information may result from consumers' decisions to veto (opt-out from) any "sale" of their personal information by a given business or the exercise of their (limited) right to have their personal information permanently deleted by the business that collected the data from the consumer. As its main policy tool, the CCPA gives consumers the right to direct businesses that collect data from the consumer to provide fairly detailed disclosures about the categories of personal information collected about a given consumer, the intended use, and the nature of third parties such PI is shared with by the collecting business. Importantly, a CCPA amendment delaying enforceability of certain individual rights by employees in a labor or business-to-business context has been grandfathered into the CPRA.

New Class of Personal Information – Sensitive Information

Although the CPRA does not fundamentally change the essential features of the CCPA, the CPRA abandons the uniform concept of personal information in favor of a split concept by creating a specially protected class of "sensitive personal information". The scope of data deemed sensitive information combines elements of the GDPR's "special categories of personal data," such as religious beliefs or political views, with certain classes of high value personal information such as driver's license numbers or banking and credit card information, or a consumer's exact geolocation.

However, contrary to the GDPR, which in essence prohibits the processing of sensitive data except in a number of narrowly defined exceptions, California consumers merely have the right to restrict a business from using such sensitive information outside what is reasonably necessary for the provision of goods or services in a given transaction.

Additional Rights and Restrictions

Mandatory Limit on Retention of Personal Information; Right of Correction.

The CCPA codifies additional fair processing principles, such as a limitation on retention of personal information and a requirement to ensure that only accurate data is processed and gives consumers the right to request that businesses correct inaccurate personal information maintained about them in certain circumstances.

Deletion Rights Extend to Supply Chain.

A consumer's right to have his or her personal information deleted is expanded throughout a collecting entity's supply chain.

Right to Opt out of Sharing of Personal Information.

The CCPA gave consumers the right to prohibit (opt-out) businesses the "sale" of personal information about a consumer. However, despite a fairly broad definition of "sale" under the CCPA, the practical implementation of this requirement revealed a number of gray areas that were, unfortunately, not addressed by the implementing regulations introduced by California Attorney General in 2019 (the final version became effective in July 2020). While certain groups and commentators prefer an extremely wide reading of the term and argue that the use of third party cookies in many instances constitutes a "sale" of personal information, some industry representatives favor an extremely narrow construction of the term.

The CPRA seeks to clarify this issue by introducing a new category, "sharing" of personal information, alongside the retained "sales" concept. The definition of "sharing" includes the providing of information for cross-context behavioral advertising and consumers may now opt out from their information being "shared or sold". This may have a significant impact on the use of personal information in the context of online advertising.

Stand-Alone Obligation to Implement and Maintain Reasonable Security Measures

The obligation to implement reasonable security measures was already part of the CCPA; however, a violation of this requirement was actionable only if it resulted in a data breach involving covered personal information. Under the CPRA, failure to maintain reasonable security procedures and practices to protect the personal information from unauthorized or illegal access destruction, use, modification or disclosure is a sanctionable violation, regardless of whether or not a data breach ensues.

Enforcement

- **Private Right of Action.** Like the CCPA, the CPRA does not include a universal private right of action for all violations. Rather, only data breaches allow for private actions. There are, however, expanded plaintiff's rights in case of a breach involving covered personal information. The definition of covered personal information has been expanded to include an email address in combination with a password and security questions and answers that would permit access to that e-mail account. Moreover, in breach scenarios, defendants' ability to avoid liability by remedying the violations at issue during a thirty-day cure period has been greatly curtailed.
- **Creation of New Enforcement Agency.** The CPRA provides for the creation of the "California Privacy Protection Agency" to take over the enforcement of the law from the Attorney General's office. The CPRA ensures that the agency has at least a $10 M budget starting in 2022 in addition to other allocations to be made as part of the regular budgeting process. This state agency is to start its operations as soon as the ballot text becomes California law and has therefore about a year to prepare before the CPRA's operative provisions become effective. Overall, the creation of a specialized agency is not necessarily bad news for business. As the example of the Data Protection Agencies in the EU shows, they can become trusted partners for both industry and consumers as they emphasize guidance over heavy-handed enforcement.

Proposition 24 has Passed – What Should Businesses Do Next?

"Ask for more money". While this advice to privacy managers attributed to a privacy pundit in a Proposition 24 roundtable may not be an accurate quote, it is indicative for the unknowns surrounding this new law. What is certain, however, is that, initially, a robust investment in

compliance will be required. While the details have yet to be fleshed out, a few specific action items have already emerged. Businesses should:

- Plan on updating their data map/ ROPA to identify and segregate "Sensitive Personal Information" from regular personal information.
- Allocate sufficient time and resources to analyze their vendor relationships to ensure that they are properly classified as service providers or contractors, if applicable, and the requisite contractual documentation is in place. If there is enough time, redundant holdouts can be replaced without significant business disruptions.
- Leverage on the experience of your EU subsidiaries or affiliates who are conducting their on-line ad tech operations in an ecosystem that is very similar to the CPRA.
- Start working on a retention schedule, if none is in place, and revise existing retention schedules to conform to the CPRA's legal requirements.

For any questions or concerns about specific situations, please feel free to contact Christian Hammerl at chammerl@mdmc-law.com, Bradford Meisel at bmeisel@mdmc-law.com, or Diane Reynolds at dreynolds@mdmc-law.com.

Offices

NEW JERSEY | NEW YORK | COLORADO | PENNSYLVANIA

CONNECTICUT | MASSACHUSETTS | DELAWARE | RHODE ISLAND | FLORIDA

Unsubscribe