MAYER | BROWN

November 13, 2020

Legal Update

What Comes Next After "Yes" on 24? From the CCPA to the CPRA and Beyond

On November 3, 2020, a majority of Californians cast "yes" votes for Proposition 24, the ballot initiative enacting the California Privacy Rights Act of 2020 (CPRA). Although the election results have not yet been certified by the California Secretary of State and may not be before December 11, 2020 (the latest date), the CPRA had reached 56-percent approval the morning after the election, causing the initiative's proponents to declare victory and opponents to concede defeat. The CPRA, of course, builds on the California Consumer Privacy Act (CCPA), which only just became effective on January 1, 2020, and then enforceable on July 1, 2020. Readers can be forgiven for CCPA-CPRA fatigue. Following the drama of the CCPA's enactment in June 2018, two legislative sessions of tense amendment negotiations, three drafts of CCPA regulations and a fourth version of the regulations potentially on the way, compliance officers and privacy professionals may be left with heads spinning. Unfortunately, the CPRA's enactment is not an end to this progression, but simply another new beginning. This Legal Update aims to provide an overview of what comes next, after the CPRA becomes official in early to mid-December 2020. Specifically, we will highlight the significant differences between the CCPA and CPRA, the institution of the new agency charged with enforcing the CPRA, the revised timeline for regulation and enforcement, and steps businesses can take to begin their compliance efforts.

Substantive Changes

The CPRA does not start from scratch but rather amends the direct language of the CCPA (beginning at California Civil Code section 1798.100), modifying some provisions, deleting others and adding new provisions altogether. Some of the amendments are merely technical or typographical, but many are substantive and significant, designed by the authors "to strengthen consumer privacy rights and prevent dilution by amendments." (For an overview of the journey from CCPA to CPRA, see our July 3, 2020, Legal Update, "A Legal Soap Opera — As the CCPA and the CPRA Turn.") The CPRA is also designed with an eye towards obtaining an "adequacy" finding under the European Union's General Data Protection Regulation (GDPR), such that compliance with the CPRA is considered to provide an adequate level of data protection for data transfer purposes under the GDPR. Here are some of the more noteworthy changes:

ESTABLISHES A NEW CATEGORY OF "SENSITIVE PERSONAL INFORMATION"

The CCPA only applies to covered businesses dealing with the personal information (PI) of California-resident consumers. The CPRA retains these benchmarks, but creates a new category of "sensitive

personal information," the collection and use of which must be separately disclosed to consumers and which otherwise receives the same protections as PI. But whereas under the CCPA, consumers can instruct a business to delete or stop selling (i.e., opt out of the sale of) their PI, under the CPRA, consumers can also direct a business to limit the use of sensitive PI to that which is necessary to perform services or provide goods. Sensitive PI includes biometric information, consumer health data, the details of a consumer's sex life or sexual orientation and PI that reveals a consumer's social security, driver's license, state ID or passport number; financial account information and credentials; precise geolocation; race, ethnicity, religious or philosophical beliefs, or union membership; mail, email or text messages intended for anyone other than the business; and genetic information.

ENHANCES RIGHTS OF OPT-OUT AND DELETION

The CPRA also enhances the aforementioned rights of opt-out and deletion. The CCPA requires businesses that sell PI to provide consumers with the right to opt-out of such sale by making a hyperlink available on the homepage of their websites under the title "Do Not Sell My Personal Information." The CPRA expands these protections to cover the "sharing" of data with third parties for cross-context behavioral (i.e., targeted) advertising, whether for money/consideration or not. While it was arguable under the CCPA whether the use of behavioral advertising was considered to be a "sale" of PI, the CPRA now makes it clear that it is. The opt-out link must be retitled "Do Not Sell or Share My Personal Information," though businesses are given the option to accept consumers' opt-out preference signals in lieu of posting the hyperlink (similar to Do Not Track/DNT signals in the web-browsing and cookie-tracking contexts).

In addition to opt-out, the CCPA requires businesses that collect PI directly from consumers to honor verifiable requests for deletion and to notify contractors and service providers to delete the consumer's PI, as well. The CPRA carries this deletion requirement further downstream, requiring businesses to notify all third parties to whom the consumer's PI has been sold or shared (for targeted advertising) to delete the PI, unless doing so would involve disproportionate effort or prove impossible.

CREATES A RIGHT TO CORRECT INACCURATE DATA AND PRINCIPLES OF PURPOSE LIMITATION, STORAGE LIMITATION AND DATA MINIMIZATION

The CPRA also grants consumers the right to request correction of inaccurate PI, and businesses must use commercially reasonable efforts to correct any such inaccuracies upon receipt of a verifiable consumer request. Further contours of the right to correction, and businesses' corresponding obligations, are to be addressed in additional regulations, including, importantly, businesses' ability to investigate and reject unsubstantiated requests.

The CCPA prevents businesses from using PI for purposes other than those disclosed in advance to consumers. The CPRA reaffirms this "purpose limitation," prohibiting businesses from using consumer PI for purposes that are incompatible with the purposes disclosed at or before collection. The CPRA also imposes a "storage limitation" on businesses, who may not retain PI for longer than is reasonably necessary to accomplish the disclosed purpose for which the PI was collected. Moreover, the CPRA mandates that a business's collection, use, sharing and retention of consumer PI must be "reasonably necessary and proportionate" to achieve the purposes for which the PI was collected or some other compatible purpose, a principle commonly known as "data minimization."

CLARIFIES AND CONFIRMS CERTAIN EXEMPTIONS

The CCPA definition of PI expressly does not include publicly available information, but the CCPA narrowly defines public data to mean merely data lawfully made available from government records. The CPRA expands this definition to include information that a business reasonably believes is lawfully

made available to the general public, either by the consumer or through widely distributed media, as well as information disclosed by the consumer without restricting the audience, such as social media profiles and postings made without enabling privacy settings. The CPRA also exempts lawfully obtained, truthful information considered a matter of public concern.

Similarly, the CCPA exempts employee/applicant PI and PI conveyed in transactions of goods and services from one business to another (B2B), where a consumer acts on behalf of one of the businesses—but these exemptions sunset (i.e., terminate) on January 1, 2022, under the CCPA. The CPRA extends the B2B and employee data exemptions to January 1, 2023, the date the CPRA becomes operative. Essentially, the CPRA gives legislators and stakeholders two more years to determine if and how the CPRA should apply to employee and B2B data.

TRIPLES PENALTIES FOR VIOLATIONS INVOLVING MINORS' DATA

Under the CCPA, businesses may be fined up to $2,500 for each violation of the Act and up to $7,500 for each intentional violation. The CPRA increases the penalty for unintentional violations involving the PI of persons under the age of 16 from $2,500 to $7,500 per violation.

The New Enforcement Agency

The CPRA is not just a change in law, but a change in who enforces the law. The CCPA includes a limited private right of action, authorizing consumers to sue only after certain of their PI is exposed due to theft, exfiltration or disclosure due to a business's failure to maintain reasonable security protocols—in other words, after a data breach. Otherwise, violations of the CCPA are investigated and enforced administratively by the California Department of Justice (DOJ) overseen by the Office of the California Attorney General (OAG). The CPRA largely leaves this enforcement regime intact, with one significant change: the DOJ will give way to the newly established California Privacy Protection Agency (the "CPP Agency"). Whereas the OAG has numerous responsibilities and had urged that it lacked the resources to adequately enforce the CCPA, the CPP Agency's sole obligation is to administer, implement and enforce the CCPA and CPRA. The CPRA transfers responsibility and authority from the OAG to the CPP Agency either on July 1, 2021, or six months after the CPP Agency indicates it is ready for transfer, whichever comes earlier.

The CPP Agency will be governed by a five-person board to be appointed by the OAG, the Senate Rules Committee and the speaker of the assembly—who each will appoint one member—and the governor, who will appoint one member and the agency chair. Board members are to be experienced in the areas of privacy and technology, particularly, and must remain free from influence, including restrictions on post-board service employment. The CPRA provides initial funding for the CPP Agency in the form of a government loan of $5 million for fiscal year 2020-21 and $10 million annually thereafter, to be repaid over time from fines and settlements collected by the CPP Agency in enforcement. Nine percent of the funds collected may be redistributed as grants for non-profit privacy organizations, law enforcement entities and schools, while the remaining 91 percent of collections are to be invested with earnings going to the state general fund. After the vote approving the CPRA is certified, the next big thing to watch for will be the appointment of the CPP Agency's board and the board's hiring of an executive director.

Regulatory Timeframe

As important as the change in substantive law is the timeline on which such changes will occur. In California (as elsewhere), there are differences between when a law becomes *effective* (when the law takes effect), *operative* (when the law must be obeyed) and *enforceable* (when the law may be

enforced). Delays between effective and operative/enforcement dates are meant to provide affected businesses and individuals with time to become acquainted with the law and to build out compliance mechanisms, and to provide regulators the opportunity to build out enforcement machinery. The results can be confusing, all the more so where, as here, a first law remains in effect while a second comes into existence, and each law contains sunsetting provisions. Over the next several years, California will have two substantive laws, two sets of regulations and two enforcement agencies—all going in and out of existence at various times or others. Keeping track of the timeline will be of utmost importance for covered businesses and privacy professionals.

As summarized in the table below, the CPRA will become effective on or before December 16, 2020—five days after the Secretary of State certifies the approving vote on or before December 11. The CPRA does not become operative, however, until January 1, 2023, and then only applies to PI collected on or after January 1, 2022 (the "lookback period"). Then still, the CPP Agency may not begin enforcing the CPRA until July 1, 2023, and then only for violations occurring on or after that date—a six-month grace period as under the CCPA. In the meantime—until the CPRA is both operative and enforceable on July 1, 2023—the CCPA (including provisions that will change when the CPRA becomes operative) and its regulations will remain in full force and effect, enforceable by the OAG and, after transition of authority, the CPP Agency. But the landscape will continue to evolve.

While the CCPA will remain operative and enforceable from now until July 1, 2023, California's privacy-law landscape will continue to evolve during that time. Significantly, the CPP Agency must file its notice of rulemaking, including new draft regulations as directed by the CPRA, by July 1, 2021. After notice, comment and any revision, those regulations must be finalized and adopted by July 1, 2022. California's Office of Administrative Law then must review and approve the final proposed regulations for conformity with the California Administrative Procedures Act. Only then will both the CPRA and its implementing regulations be effective, though attempts may yet be made to amend the CPRA further, such as to formalize the B2B and employee data exemptions set to expire January 1, 2023.

Date	Event	Date	Event
Jan. 1, 2020	CCPA effective	**By March 2021**	CPP Agency appointed
July 1, 2020	CCPA enforceable	**By July 1, 2021**	CPP Agency assumes authority and proposes CPRA regulations
Aug. 14, 2020	CCPA regulations enforceable	**By July 1, 2022**	CPRA regulations to be adopted
Nov. 3, 2020	"Yes" vote on Prop 24	**Jan. 1, 2023**	CPRA operative[2]
By Dec. 16, 2020	CPRA effective[1]	**July 1, 2023**	CPRA and CPRA regulations enforceable[3]

[1] CCPA and regulations remain operative and enforceable from present until July 1, 2023.

[2] CPRA is operative January 1, 2023, but only covers data dating back to January 1, 2022.

[3] CPRA and regulations are enforceable July 1, 2023, but only for violations thereafter.

What To Do Next

Readers should pay close attention to these developments outlined in the calendar above and check back for updates on what comes next after California's "yes" vote on Proposition 24. In the meantime, we highlight a few steps businesses can consider taking now to begin complying with the CPRA.

REVIEW AND EXPAND INTERNAL PROCESSES

Consumer Requests. Businesses should review their internal processes for handling consumer requests and identify how to expand such processes to enable consumers to do the following:

- Limit the use and disclosure of sensitive PI to uses that are necessary to perform the business purpose for which the sensitive PI was collected; and
- Correct inaccurate PI after receiving a verifiable consumer request.

Purpose Limitation, Storage Limitation and Data Minimization. Businesses should evaluate how they use PI, confirm the purposes for collecting and processing such PI, and review their data retention practices to ensure compliance with the purpose limitation, storage limitation and data minimization principles as described under the CPRA.

WEBSITE LINKS AND PRIVACY NOTICE

Website Links. As previously mentioned, the CPRA expands the right to opt-out of a "sale" of PI to include "sharing" of PI with third parties for cross-context behavioral (i.e., targeted) advertising. Therefore, businesses should update their "Do Not Sell My Personal Information" link to "Do Not Sell or Share My Personal Information" and enable opt-outs through such link to also opt out the user of any behavioral advertising. Alternatively, a business may consider whether it is feasible to accept consumers' opt-out preference signals in lieu of posting the hyperlink. Further, because the CPRA provides consumers with the right to limit businesses from using and disclosing their sensitive PI, businesses should consider whether to provide a new link titled "Limit the Use of My Sensitive Personal Information" or combine this right with the "Do Not Sell or Share My Personal Information" link.

Privacy Notice. Businesses should review and consider what updates should be made to their initial notice at collection and website privacy notice to reflect new requirements, including those concerning sensitive PI and the new or expanded consumer rights. With respect to sensitive PI, businesses must provide a separate disclosure regarding sensitive PI that describes the categories of sensitive PI collected, the purposes for which the categories of sensitive PI are collected and used, and whether such sensitive PI is sold or shared. Given the new requirement, businesses should take an inventory of the PI that they collect and identify whether such PI is sensitive PI. In addition, businesses should review their use of sensitive PI and ensure such use is compliant with the standards in the CPRA.

CONTRACTS WITH SERVICE PROVIDERS

Businesses should review their contracts with service providers and contractors and update those contracts to reflect the contractual provisions the CPRA requires businesses to include. Some of the new provisions that the CPRA requires to be included in contracts include: (i) specifying that the PI is sold or disclosed only for limited and specified purposes; (ii) obligating such parties to comply with applicable obligations under the CPRA; (iii) obligating such parties to provide the same level of privacy protection as the business is required to provide under the CPRA; and (iv) requiring such parties to notify the business if it can no longer meet its obligations under the CPRA.

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

Philip R. Recht
+1 213 229 9512
precht@mayerbrown.com

Evan M. Wooten
+1 213 621 9450
ewooten@mayerbrown.com

Lei Shen
+1 312 701 8852
lshen@mayerbrown.com

Annemarie S. Kong
+1 312 701 8304
askong@mayerbrown.com