June 26, 2020

New California Privacy Initiative Certified for November Ballot

Attorneys
Edward R. McNicholas
Judith G. Rubin

On November 3, 2020, Californians will vote on whether to approve a ballot initiative to enact a new California Privacy Rights Act (CPRA). If, as current polling suggests, California voters pass the CPRA into law in November, it will significantly revise the California Consumer Privacy Act (CCPA) of 2018, which entered into force only in January of this year.

The CPRA expands the provisions of the CCPA, removes the ability of businesses to remedy some violations before they are penalized, and creates a new agency – the California Privacy Protection Agency – to implement and enforce it. The CPRA's substantive provisions would take effect on January 1, 2023, but its new obligations would apply to personal information collected after January 1, 2022.

Uncertainty will no doubt continue to be a constant aspect of California privacy law for the foreseeable future with this new "CCPA 2.0." On a practical matter, companies may wish to begin planning for substantive compliance with the CPRA's provisions, as some may involve significant information systems design and engineering in addition to policy and procedure revision. Companies covered by the federal Gramm-Leach-Bliley Act or HIPAA, however, may well avoid some of the impacts that will be very significant for other sectors of the economy.

Background

In early 2018, after several unsuccessful attempts by the California legislature to pass comprehensive privacy legislation, a real estate investor named Alistair Mactaggart spearheaded and financed an initiative that sought to include a new data privacy law on the November 2018 California ballot. The initiative, backed by a Mactaggart non-profit called Californians for Consumer Privacy, gained enough support to collect the necessary signatures to be certified to the ballot. Concerned about widespread criticism of the new law as too broad and unworkable, and in order to avoid the passage of a law that would be difficult to amend,[1] California lawmakers worked with Mactaggart's initiative to find a compromise. As a result, a substitute bill, the CCPA, was passed after only a few days of intense debate, and the ballot initiative was withdrawn.

The CPRA is the second ballot initiative from Mactaggart's non-profit. Under the slogan "It's your personal information, take back control!" the initiative is premised on the idea that the CCPA does not sufficiently protect the privacy of consumers from "giant corporations." On May 4, 2020, just in time to qualify the initiative for the 2020 ballot, Californians for Consumer Privacy submitted over 900,000 signatures in support of the CPRA. Satellite litigation between the Californians for Consumer Privacy and the Secretary of State ensued over the timing of the process for verifying signatures, but on June 25, 2020, the Secretary of State certified the initiative as qualified for the November 3, 2020, General Election ballot.

Since the Secretary of State has certified the measure, it is now no longer a "proposed" initiative and can no longer be withdrawn[2] – a last-minute compromise like with the CCPA in 2018 is thus not an option. Californians for Consumer Privacy claims that a fall 2019 survey shows that nearly 9 out of 10 California voters supported the measure.[3] Whether such overwhelming support shows up at the polls remains to be seen, but the fact that the measure is now on the ballot will likely increase demands for other California privacy laws or a federal privacy law. That numerous other states are considering enacting their own privacy laws makes this situation even more pressing, even as several state privacy initiatives have apparently been paused or collapsed in light of the urgency of pandemic legislation. Considering that the CPRA provides for a time lag of two years between its adoption and the effectiveness of most of its provisions, federal legislators may have both the incentive and the time to enact a countrywide privacy law after the November election.

Scope

Definition of "Business"

As with the CCPA, the CPRA covers a business that collects the personal information of California residents, but it revises some of the definitions of "business." Among other things, it increases one of the thresholds that a business must meet in order to be covered by the CPRA. A company now needs to buy, sell or share the personal information of 100,000 (instead of 50,000) consumers or households per year to be considered a "business" under the CPRA.[4]

Employee and Business-to-Business Exemptions

The CPRA retains the CCPA's exemptions for personal information collected in the employment and certain business-to-business contexts until January 1, 2023. These exemptions are currently scheduled to become inoperative on January 1, 2021.[5]

GLBA Exemption

The CPRA slightly rephrases the CCPA's GLBA exemption. The CPRA would not apply to "personal information collected, processed, sold, or disclosed "*subject to*" the GLBA, instead of "*pursuant to*" the GLBA.[6] This may be a response to some commentators who read "pursuant to" as particularly narrow, although our understanding is that the drafters intended "pursuant to" to be read as "subject to" already.

Purpose Limitation – Necessity and Proportionality

In a new provision that relates to all aspects of business's handling of personal information, the CPRA creates a new, GDPR-style purpose limitation, which the AG regulations already contemplate. It provides that a business's collection, use, retention, and sharing of personal information be "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes."[7] Any interaction of a business with a consumer's personal information will thus have to be assessed through the lens of necessity and proportionality – which is a routine step under EU privacy but novel in the U.S. and in some considerable tension with First Amendment freedom for commercial speech.

Third Parties

The CPRA imposes additional obligations on service providers, contractors and other third parties who have received personal information from California businesses. Businesses must enter into written agreements with such third parties that require them to comply with the CPRA.[8] Moreover, if a business receives a deletion request from a consumer, it would need to notify all third parties with whom it has shared personal information,[9] and those third parties would be obliged (with certain exceptions) to assist with, and comply with, the request.[10]

Additional Protection of Sensitive Personal Information (SPI)

The CPRA creates a new category of Sensitive Personal Information (SPI), which receives additional protections. It includes consumers' "precise" geolocation, the content of emails or text messages, philosophical or religious beliefs, information collected and analyzed concerning a consumer's health or sex life, and account log-in or financial information in combination with the required access or security code.[11] This definition could be significant, as it would impact several technologies that are important for the advertising industry and companies who advertise to consumers.

Under the CPRA, consumers have the right to request that a business limit the use or disclosure of their SPI to "that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer," or as authorized by certain regulations, unless they provide consumers with the right to limit additional uses or disclosures.[12] Moreover, businesses would need consumer consent prior to the sale of SPI.[13] Whether such opt-in requirement would

survive First Amendment scrutiny, however, would remain to be seen in light of *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011).[14]

Right to Opt Out of Sale and Sharing

Another provision also takes aim at the online advertising industry. While the CCPA provided consumers with the right to opt out of the "sale" of their personal information, the CPRA extends this to any "sharing" of personal information. Importantly, "sharing" is defined as 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."[15] The CPRA describes how businesses would be required to enable consumers to opt out, potentially limiting the use of behavioral advertising.

Right to Know

The CCPA limits the disclosure of information under the "Right to Know" to the 12-month period before the respective request was received. The CPRA extends this window for personal information collected on or after January 1, 2022 beyond that 12-month period, if the consumer requests this and "unless doing so proves impossible or would involve a disproportionate effort."[16]

In order to comply with this obligation, a business needs to provide the consumer with the categories of personal information, the categories of sources, the purposes for collecting, selling or sharing the personal information, and the categories of third parties to whom the information is or has been disclosed.[17] The information needs to be provided in an easily understandable and, if technically feasible, machine-readable format – which creates an equivalent to the EU right of portability.[18]

Right to Correct

The CPRA would create a new right to correction for consumers.[19] Under this provision, businesses must use commercially reasonable efforts to correct inaccurate personal information, taking into account "the nature of the personal information and the purposes of the processing of the personal information." As in the case of consumers exercising their right to know or to delete, the business would need to be presented with a verifiable consumer request.

Requirement to Delete

One of the most significant new obligations for businesses relates to data retention. The CPRA would require businesses to inform consumers at or before the point of data collection of "the length of time [it] intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine such period."[20] Moreover, businesses would not be allowed to retain personal information "for longer than is reasonably necessary" for the purpose for which the collection was disclosed.[21]

The CPRA also modifies the CCPA's right to deletion. In response to a verifiable deletion request, businesses must now notify third parties to whom the business has sold or with whom it has shared personal information to delete it. Subject to certain exemptions, service providers and contractors are required to cooperate and to delete personal information when directed.[22]

While complying with data retention and deletion best practices considerably limits the damage of data breaches, many companies struggle with their implementation. This obligation could serve as an additional incentive to regularly delete personal information that is no longer needed.

More Protection for Children's Data

The CPRA states that if a consumer under 16 does not provide consent to the selling or sharing of his or her personal information, businesses may not repeat such request for consent for at least 12 months.[23] It also calls for regulations establishing the technical specifications for opt-out signals for individuals under the age of 13, or between 13 and 16.[24]

Finally, the CPRA would increase the administrative fines for violations of children's personal information to three times the amount of those for adults ($7,500 per violation), if the business had actual knowledge that the consumer was under 16 years old.[25]

Automated Decision-Making

In a provision that echoes the GDPR and may inhibit the deployment of AI, the CPRA defines "profiling" and creates new access and opt-out rights[26] related to automated decision-making. "Profiling" is defined as "any form of automated processing of personal information […] to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."[27] The Attorney General is tasked with adopting regulations to govern access and the right to opt out, including how to respond with "meaningful information about the logic involved in such decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer."[28]

Audits and Risk-Assessments

Again echoing the GDPR, the CPRA would task the Attorney General with the adoption of regulations that require businesses whose "processing of consumers' personal information presents significant risk to consumers' privacy or security" to perform annual privacy and data security audits. The Attorney General, and then the new California Privacy Protection Agency (CPPA), would be required to issue regulations requiring annual audits and regular risk assessments by businesses that undertake high-risk processing. What determines such high-risk activities would depend both on the size and complexity of the business, and the nature and scope of the processing. The regulations would require the respective businesses to perform yearly thorough and independent cybersecurity audits, and to submit regular risk assessments to the CPPA. These risk assessments would need to mention whether the processing involves sensitive personal information, and weigh "the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer" and "the goal of restricting or prohibiting such processing if the risks […] outweigh the benefits" for the respective stakeholders.[29] The regulations would need to be adopted by January 1, 2022.[30]

Reasonable Security Procedures and Practices and Expanded Liability for Breaches

The CCPA introduced a private right of action, accompanied by statutory damages, for data security incidents that result from a business's violation of its duty to "implement and maintain reasonable procedures and practices appropriate to the nature of the information." The CPRA explicitly reaffirms the duty to implement such measures.[31]

Presently, under the CCPA, consumers can pursue the private right of action if a data breach exposes their first names or initials and last names, combined with certain other elements like social security numbers or bank accounts. The CPRA adds to this the combination of consumers' e-mail addresses and passwords.[32] Considering the frequency of such breaches, the effect of this addition could be considerable. Moreover, the CPRA eliminates the possibility to "cure" for a data breach after the fact if a business implements and maintains reasonable security practices and procedures within 30 days,[33] which the CCPA allows.

While neither the CCPA nor its draft regulations provide guidance on the term "reasonable," the concept of reasonable security practices is not new to California law. In 2016, for example, the Attorney General at the time provided a comprehensive analysis of data breaches and cybersecurity recommendations. It declared the set of 20 data security controls published by the Center for Internet Security (CIS) "a minimum level of information security that all organizations that collect or maintain personal information should meet." Other authoritative information security standards mentioned by the report include those published by the National Institute of Standards and Technology (NIST), and the International Organization for Standardization (ISO).

Establishment of the California Privacy Protection Agency

With the establishment of the California Privacy Protection Agency (CPPA),[34] the CPRA would create the first agency in the U.S. that is exclusively dedicated to privacy. The CPPA is to be vested with the power to "administer, implement and enforce" the CPRA through administrative actions,[35] and have investigative,[36] subpoena[37] and audit[38] powers. It could impose administrative fines of up to $2,500 per violation of the CPRA or up to $7,500 per intentional violation or violations involving the personal information of minors.[39] Eventually, the CPPA would take over the rulemaking authority from the Attorney General's Office.[40] Other tasks would be to build public awareness and understanding about privacy risks,[41] provide guidance to consumers[42] and businesses,[43] and (upon request) provide technical assistance and advice to the legislature.[44]

The CPPA would receive an initial funding of $5 million in the fiscal year 2020-2021, and $10 million in annual funding thereafter.[45]

Entry into Force

As a general matter, the CPRA's new provisions would come into effect five days after the Secretary of State certifies the election results.[46] CPRA section 31, however, provides that most of its provisions will become operative on January 1, 2023, and shall (except with regard to the right to access) apply only to personal information collected on or after January 1, 2022. Until this time, the CCPA shall remain in effect.

A few provisions will become effective on the date of the Act. They include the above-mentioned extension of the CCPA's employee and business-to-business exceptions, many of the provisions governing the establishment of a California Privacy Protection Agency,[47] and the Attorney General's mandate to adopt regulations.[48]

Outlook

Companies that have already undergone the process of becoming GDPR- or CCPA-compliant will find many familiar obligations in the CPRA. Such businesses will generally be in a good position to adapt their compliance, where necessary, to the new requirements. Three aspects, however, may require additional attention.

Data Retention

The CPRA's requirements regarding the obligations of businesses to inform consumers about their data retention practices have no equivalence in the CCPA and go beyond any similar obligations under the GDPR. Businesses would be required to inform consumers at the time they collect their personal information (or before) about their data retention practices for each category of personal information.

The required level of detail may, effectively, equal the granularity of an organization's internal data retention policy – and may well require companies to be much more attentive to data retention *and* defensible deletion polices. While maintaining and adhering to data retention policies is privacy best practice and significantly limits an organization's exposure in case of a data breach, it is a practice that challenges many organizations.

Behavioral Advertising

The CCPA does not limit behavioral advertising if it can be done without "selling" the data, but the CPRA seems to target behavioral advertising more widely. Similar to the situation under the GDPR and the ePrivacy Directive, however, many terms remain unclear and open to interpretation. One aspect is that "sharing" of personal information, which does not require monetary or other valuable consideration, is, like "selling," subject to consumers' opt-out requests. A business that receives such a request is prohibited from using the personal information outside their business relationship.[49] This might include "cross-context behavioral advertising" as a service with which a consumer does not intentionally interact.[50] If the CPRA is passed into law, it may be for the new CPPA regulator to engage with the industry to find constructive pathways forward.

Designation of Account Log-in and Passwords as SPI

Declaring the combination of an account log-in and the respective password as SPI is particularly important because it implicates common "credential stuffing" cyberattacks. Such attackers operate on the assumption that many users use the same log-in names and passwords across systems. The attack thus uses lists of compromised user data (often obtained from another data breach) to direct large-scale automated log-in requests against a web application to gain access to user accounts. This can result in data breach notification obligations, investigations, and class actions – even in circumstances where the companies' own systems were not breached but responded as designed to stolen credentials.

For more insights on the CCPA and other data, privacy and cybersecurity related topics, visit our blog at www.RopesDataPhiles.com.

1. Under the peculiarities of California law, initiatives that pass via the ballot process are much more difficult to amend, modify, or repeal, than other bills. They usually require either another initiative or a 70% majority in the California legislature.
2. *See* California Elections Code §§ 9033, 9604.
3. *See* https://www.caprivacy.org/icymi-summary-of-key-findings-from-california-privacy-survey/.
4. CPRA Section 1798.140(d)(B).
5. CPRA Section 1798.145(m) and (n).
6. CPRA Section 1798.145(e).
7. CPRA Section 1798.100(c).
8. CPRA Section 1798.100(d).
9. CPRA Section 1798.105(c)(1).
10. CPRA Section 1798.105(c)(3), 1798.105(d).
11. CPRA Section 1798.140(ae).
12. CPRA Section 1798.121(a).
13. CPRA Section 1798.121(b).
14. In this case, the U.S. Supreme Court struck down as a violation of the First Amendment Vermont's Prescription Confidentiality Law, which restricted the sale, disclosure, and use of records that revealed the prescribing practices of individual doctors.
15. CPRA Section 1798.140(ah).
16. CPRA Section 1798.130(a)(2)(B).
17. CPRA Section 1798.130(a)(3)(B)(ii).
18. CPRA Section 1798.130(a)(3)(B) (iii).
19. CPRA Section 1798.106.
20. CPRA Section 1798.100(3).
21. CPRA Section 1798.100(3).
22. CPRA Section 1798.105.
23. CPRA Section 1798.135(c)(B)(5).
24. CPRA Section 1798.185(a)(19)(B).
25. CPRA Section 1798.155(a).
26. CPRA Section 1798.185(a)(16).
27. CPRA Section 1798.140 (z).

28. CPRA Section 1798.185(a) (16).
29. CPRA Section 1798.185(a)(15).
30. CPRA Section 1798.185(d).
31. CPRA Section 1798.100(e).
32. CPRA Section 1798.150(a)(1).
33. CPRA Section 1798.150(b).
34. CPRA Section 1798.199.10 ff.
35. CPRA Section 1798.199.40(a).
36. CPRA Section 1798.199.45.
37. CPRA Section 1798.199.65.
38. CPRA Section 1798.185(a)(15).
39. CPRA Section 1798.199.55(a), 1798.155.
40. CPRA Section 1798.185 (d) states: "Beginning the later of July 1, 2021, or six months after the Agency provides notice to the Attorney General that it is prepared to begin rulemaking under this title, the authority assigned to the Attorney General to adopt regulations under this section shall be exercised by the California Privacy Protection Agency."
41. CPRA Section 1798.199.40(d).
42. CPRA Section 1798.199.40(e).
43. CPRA Section 1798.199.40(f).
44. CPRA Section 1798.199.40(g).
45. CPRA Section 1798.199.95(a).
46. *See* Cal. Const. art II section 10(a).
47. CPRA Section 1798.199.10 through 1798.199.40.
48. CPRA Section 1798.185.
49. CPRA Section 1798.135(f).
50. CPRA Section 1798.140(k).