Analysis

California Privacy Reboot Puts Rights in Spotlight

Mark E. Smith
CIPP/US, CIPP/C, CIPM
Bloomberg Law Legal Analyst

Bloomberg Law

California Privacy Reboot Puts Rights in Spotlight

By Mark E. Smith, CIPP/US, CIPP/C, CIPM, Bloomberg Law Legal Analyst

The start of the new year marked the first anniversary of the effective date of the California Consumer Privacy Act (CCPA), yet businesses are already making preparations for the voter-approved update: the California Privacy Rights Act (CPRA). The rapid evolution of California's law from one about "Consumer Privacy" to one addressing "Privacy Rights" underscores the influence of the European Union model, which recognizes privacy as a fundamental right that goes beyond commercial transactions.

While the CPRA itself does not expand privacy rights outside the commercial context–indeed, it extends the CCPA's exemptions for employee-related information and certain business-to-business communications–it should not be forgotten that California's constitution specifically recognizes privacy as an "inalienable" right (Article 1, § 1), and it is the only state constitution to elevate privacy to such a status.

As other states strive to follow California's lead on privacy, their proposals may adopt the "rights" language found in California's law, even though their respective constitutions do not expressly address privacy as a fundamental or inalienable right.

Since California, however, does recognize privacy as inalienable, any interpretation or elaboration of that right–especially where, like the CPRA, it is made by the citizens via ballot initiative–takes on added significance. And even though the CPRA, unlike many ballot initiatives, specifically provides that its provisions may be amended by a simple majority vote in the state legislature, any such amendment must be "consistent with and further the purpose and intent" of the act.

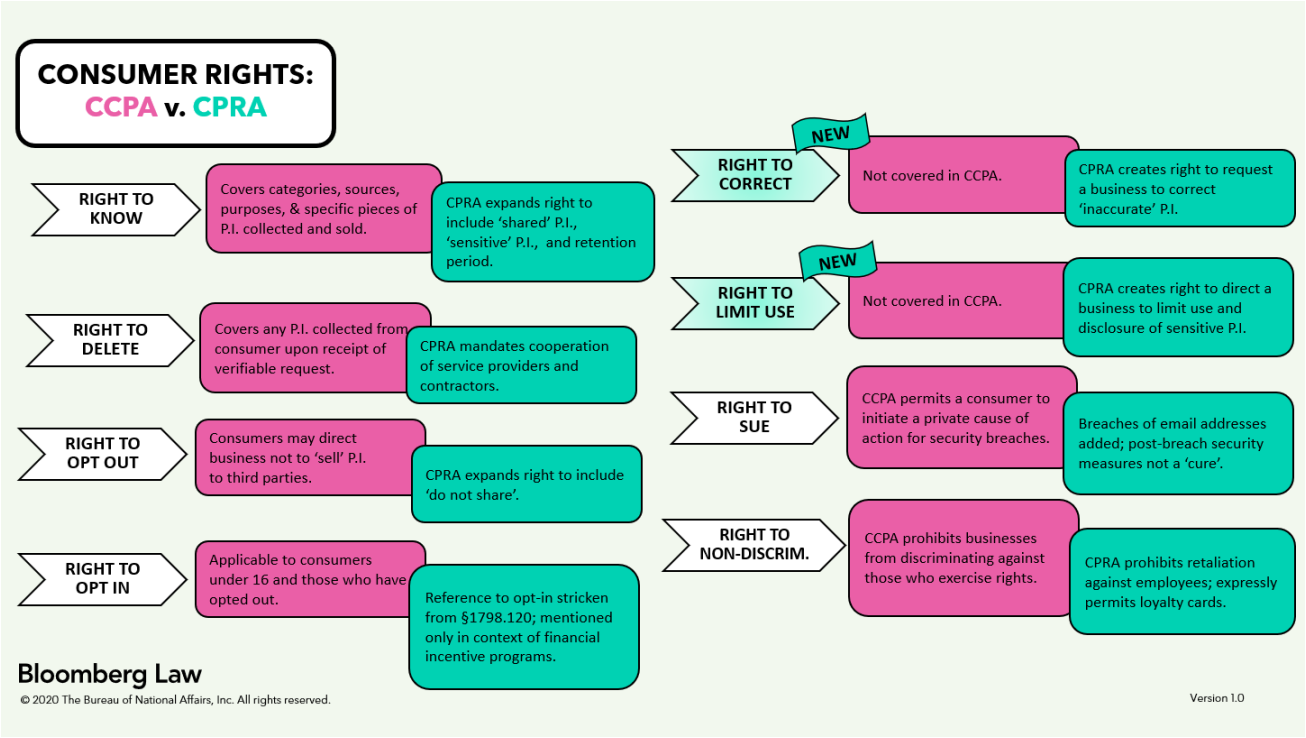
In short, California's consumer privacy rights, as enhanced by the CPRA, are very likely here to stay.

No Restriction on 'Consumer'

When the CCPA was passed in 2018, many critics argued that a "consumer privacy" law should only protect "consumers" in the context of a commercial transaction. The CCPA, however, defined a "consumer" as any California resident.

That dispute led to the adoption of the exemptions for personal information collected in the employment context and in certain B2B transactions. And, as mentioned above, the CPRA retains those exemptions, but they are set to expire on Jan. 1, 2023. That delay gives the legislature a little less than two years to extend the sunset again or make the exemptions permanent.

While a new definition of "consumer" might have been expected in a privacy regime reboot, alas, the CPRA retains the CCPA's definition. Consequently, any "consumer rights" specified in the CPRA will continue to apply to all California residents.



Right to Know

The CCPA entitles a consumer to know about the categories and specific pieces of personal information collected and sold by a business. The CPRA expands that right by entitling consumers to know about the "sharing" of personal information as well.

As I mentioned in my last piece, "sharing" refers to the transfer of personal information in the context of behavioral advertising. And unlike "selling," which refers to the transfer of personal information "for monetary or other valuable consideration," "sharing" does not require the exchange of consideration, monetary or otherwise. Rather, it encompasses the transfer of personal information to third parties in order to facilitate advertising based on the consumer's internet activity.

Since the CPRA amends each mention of "selling" with "selling *or sharing,*" the scope of the right to know is significantly expanded.

Moreover, the right to know has been updated to include the new subcategory of "sensitive personal information," also discussed in my last piece.

Intertwined with the consumer's right to know is the business's obligation to inform consumers about its collection and selling practices, which the CPRA predictably amends to require the disclosure of sharing practices.

Who's in Control?

Beyond the duty to disclose sharing practices, the CPRA makes a subtle change to the type of action that triggers the disclosure obligation.

Whereas the CCPA obliges a business that "collects" personal information to notify consumers, regardless of when that information is collected, the CPRA obliges a business that "controls the collection" to notify consumers of the categories of personal information to be collected at or before the point of collection.

"Controls the collection" is a new concept in the CPRA and one that (unfortunately) is not defined.

It's possible that more than one business may "control" the collection and therefore be required to comply with the notification requirement. For example, if a retail business includes a social media plug-in (such as a Facebook "like" or "share" button) on its website, and that plug-in collects personal information that the retailer doesn't collect on its own, the retailer could be regarded as one who "controls the collection" of that information because it added the plug-in to its website.

Facebook could also be viewed as one who "controls the collection" because it's the one who uses the information. To borrow a term from the EU's General Data Protection Regulation (GDPR), the retailer and Facebook could be viewed as "joint controllers," as in last year's *Fashion ID* judgment from the Court of Justice of the European Union (CJEU).

In *Fashion ID*, an online clothing retailer had embedded Facebook's "like" button on its website. By so doing, the retailer transmitted to Facebook the IP address of any visitor to the retailer's site, as well as technical data from the visitor's browser. This transmission occurred regardless of whether the visitor had a Facebook account or whether the visitor had clicked the "like" button.

The CJEU noted that, by embedding the "like" button, the retailer had exerted "a decisive influence over the collection and transmission of the personal data of visitors … which would not have occurred without that plugin." As such, the retailer was a controller, even though it did not itself have access to that data. Moreover, it had a duty to inform and obtain consent from visitors about the data transferred.

The same reasoning could apply to the CPRA. While the CPRA does not adopt the GDPR's concept of "joint controllers," it does recognize the concept of a "third-party business," i.e., one with whom a consumer does not intentionally interact. If Facebook is able to collect personal information from California consumers who visit the retailer's website, the consumer's right to know under the CPRA arguably applies to the retailer as well as to Facebook.

The CPRA provides that a business "acting as a third party that controls the collection of personal information" may satisfy its notice obligation by placing the notice of collection "prominently and conspicuously on the homepage of its internet

website." But how would such a notice benefit consumers accessing the retail site? Indeed, even if the retailer were to display a notice at collection saying that Facebook "controls the collection" of personal information the retailer itself does not use, would the retailer be obliged to refer consumers to Facebook's homepage to view Facebook's separate notice?

Curiously, the CPRA contains no additional references to a business that "controls the collection" of personal information. All other parts of the law refer simply to a business that "collects" personal information.

Data Retention

The CPRA also strengthens consumers' right to know as it relates to data retention. The law requires businesses to include, in the notice at collection, the retention period for each category of personal information collected, including sensitive personal information—or, if that's not possible, the criteria used to determine how long the information will be kept.

Right to Delete

As with the CCPA, the CPRA grants consumers the right to request deletion of personal information—but both laws limit that right to information a business has *collected from the consumer*.

However, since there's no indication that such a collection must arise from a consumer's *intentional* interaction, the right to delete arguably encompasses information collected by a third-party business (such as in the Facebook example above). The CPRA even clarifies that the obligation to delete extends to service providers and contractors, as well as additional downstream users, "unless this proves impossible or involves disproportionate effort."

Curiously, a service provider or contractor is not required to comply with deletion requests submitted directly to them, at least to the extent that they have collected, used, processed, or retained the consumer's personal information in their role as a service provider or contractor to the business.

Moreover, the CPRA adds a bit of wiggle room to the compliance obligation by adding the word "reasonably" to the list of exemptions: A business, service provider, or contractor is not required to comply with a deletion request if it is "reasonably" necessary to keep the information for various reasons.

The CPRA also broadens the exemption for personal information related to scientific, historical, or statistical research. Such research no longer needs to be "in the public interest."

Right to Opt Out

Unsurprisingly, the CPRA amends the right to opt out of the sale of personal information to include the right to opt out of the "sharing" of personal information as well.

Given that, the business's "do not sell" link must be updated to say: "Do Not Sell *or Share* My Personal Information."

Right to Opt In

The specific reference to the "right to opt in," found in Cal. Civ. Code § 1798.120(c), has been stricken from the CPRA, but the basis for exercising the right has not changed. So consumers under the age of 16 must "affirmatively authorize" the sale of personal information, which the CPRA expands to account for the "sharing" of personal information as well.

Opt-in language is retained, however, in the context of financial incentive programs, requiring consumers to give a business "prior opt-in consent" before providing personal information as part of a loyalty or rewards program.

Right to Private Cause of Action

The CPRA retains the private right of action for security breaches, and it adjusts the scope of the type of "personal information" that must be the subject of the breach.

Those familiar with the CCPA's private right of action are aware that, in the private cause of action context, the definition of "personal information" is the one found in subsection (d)(1)(A) of California's data security law (Cal. Civ. Code §1798.81.5), not the definition found in the CCPA . Curiously, the CCPA did not include "personal information" as defined in the following clause (subsection (d)(1)(B))—i.e., "a username or email address together with a password or security question and answer that would permit access to an online account."

The CPRA attempts to correct this anomaly by specifically adding "email address in combination with a password or security question and answer that would permit access to the account" to the scope of personal information that may be the subject of a private cause of action. It fails, however, to mention "username," so the scope as modified is still not perfectly aligned with the data security law.

The CPRA also makes another clarification regarding a business's opportunity to cure: "The implementation and maintenance of reasonable security procedures and practices pursuant to Section 1798.81.5 *following a breach* does not constitute a cure with respect to that breach." (Emphasis added.)

Right to Correct

The CPRA creates a new consumer right to request a business to correct "inaccurate" personal information if the business "maintains inaccurate information" about the consumer. Consumers must exercise the right by means of a verifiable consumer request, but the duty to correct does not appear to extend beyond the business. In other words, if a business has disclosed or otherwise shared inaccurate personal information with third parties, there doesn't appear to be an obligation for the business to notify those third parties of the inaccuracy and corresponding correction.

"Inaccurate" is not defined, however, so there could be a dispute over what's considered accurate or inaccurate. For example, if I purchase a gift for a friend—and it's something I wouldn't purchase for myself—the fact that I made the purchase would be accurate, but the inference that I would like similar items would be inaccurate. Would I be entitled to file a request to correct an inference? And how would such a request be carried out?

The CPRA requires a business to use "commercially reasonable efforts" to correct inaccurate personal information. Since it's reasonable to assume that a purchaser of one item may be interested in something similar, one could argue that correcting an inaccurate inference might be deemed commercially unreasonable.

Right to Limit Use and Disclosure of SPI

The CPRA creates another new right pertaining exclusively to sensitive personal information (SPI). If a business collects SPI, the consumer has the right to direct the business to limit its use of SPI to what's necessary or reasonably expected in order to perform the service or provide the goods.

To the extent that a business uses or discloses SPI beyond what's necessary or reasonably expected, the business now must provide notice to the consumer of the additional, specified purposes and of the right to limit that use or disclosure.

The business must also provide a "clear and conspicuous link" on the business's internet homepage, titled "Limit the Use of My Sensitive Personal Information."

However, if SPI is collected or processed "without the purpose of inferring characteristics about a consumer," the above provisions would not apply.

So it appears that if, for example, a business collects my precise geolocation information (which is SPI) in order to show me nearby restaurants (as I requested)—and not to infer whether I prefer Italian or Indian cuisine—then the precise geolocation information would be treated as ordinary personal information, subject to the other provisions of the CPRA.

Right to Non-Discrimination

The scope of the prohibition against discrimination for exercising consumer rights naturally broadens with the CPRA's addition of two new rights: the right to correct and the right to limit use. But the CPRA makes other changes as well.

First, it specifically prohibits retaliation against an employee, applicant for employment, or independent contractor for exercising their rights. It's important to note that the exemption for personal information collected in the employment context will expire on Jan. 1, 2023, when the bulk of the CPRA becomes operational.

Second, a new provision expressly states that the right to non-discrimination does not prohibit a business "from offering loyalty, rewards, premium features, discounts, or club card programs consistent with this title."

Conclusion

All in all, the CPRA enhances rights already existing in the CCPA and creates two new ones as well. Bills recently introduced in Minnesota (HF36) and New York (S567 and A680) incorporate similar consumer rights in their respective proposals.

As privacy rights are created and enhanced in the states, the prospect of a federal law with a preemption provision grows dim. The elimination of federal preemption may be one way to build "consensus" around a privacy bill in a Democratic-majority Congress, but businesses will likely push back for a single federal standard. Whether California's approval of the CPRA has unwittingly quashed any hope for a federal solution remains to be seen.

For more Bloomberg Law Analysis, visit https://news.bloomberglaw.com/bloomberg-law-analysis/.