

**LEGAL UPDATES**

# The California Privacy Rights Act: CCPA Part Two

As if businesses did not already have enough to address with the COVID-19 pandemic and compliance with the California Consumer Privacy Act (the “CCPA”), businesses need to consider the California Privacy Rights Act (the “CPRA”), which will almost certainly be on the November ballot. Structured as an amendment to the CCPA and also known as “CCPA 2.0”, the CPRA ballot initiative was spawned by Alastair Mactaggart.

06/22/2022 | 2 minute read

By [Chiara Portner](#)

As if businesses did not already have enough to address with the COVID-19 pandemic and compliance with the California Consumer Privacy Act (the “CCPA”), businesses need to consider the California Privacy Rights Act (the “CPRA”), which will almost certainly be on the November ballot. Structured as an amendment to the CCPA and also known as “CCPA 2.0”, the CPRA ballot initiative was spawned by Alastair Mactaggart. You may recall Mr. Mactaggart as the real estate developer who submitted a ballot initiative that resulted in a negotiation with the state legislature to replace the initiative with the CCPA. If the CPRA is passed and becomes law, it would be effective and enforceable January 1, 2023, with certain provisions having a look back provision.

The CPRA would establish a new category of “sensitive data” that is reminiscent of the GDPR’s definition of special categories of data but it is much broader. The definition is overly-inclusive, spanning from race, religion, and sexual orientation to financial account information and government identifiers (e.g., social security numbers). Consumers could choose to limit the use, sale and sharing of their sensitive data. Additional links on business websites may be required to “Limit the Use of My Sensitive Personal Information” in addition to the current “Do Not Sell My Personal Information” link that some businesses must now include under the CCPA.

Service providers would become directly liable for complying with certain portions of the CPRA. In particular, service providers would be required to cooperate with businesses in honoring consumer rights and to agree to maintain the same level of privacy as required by the CPRA and the CCPA.

The CPRA also adds a definition of “share” to expressly address lingering confusion over “sales” of personal information under the CCPA – and to ward off further arguments that sharing personal information for behavioral advertising in the adtech space is not a “sale” under the CCPA. Setting the record straight once and for all where the CCPA and implementing regulations have failed, “sharing” would include any provision or transfer to a third party for “cross-context behavioral advertising, whether or not for monetary or other valuable

## Related People

### Chiara Portner, CIPP/US

Partner

Redwood Shores

650.804.7672

[chiara.portner@lathropgpm.com](mailto:chiara.portner@lathropgpm.com)

---

## Related Services

[Data Privacy & Cybersecurity Compliance](#)

---

## Related Sectors

[Retail & E-Commerce](#)



consideration." Consumers would have rights to opt-out of having their information shared or sold and the "Do Not Sell My Personal Information" link would be expanded to "Do Not Sell or Share My Personal Information."

Security mandates are also increased under the CPRA, which enlarges the scope of data security breaches to include unauthorized access to or disclosure of an email address and password or security question that would allow access to an account. If the breach were attributable to the business not maintaining reasonable security measures, consumers could bring private rights of action for these breaches. Businesses that conduct higher risk processing of certain personal information would be required to undergo annual audits, thereby putting more teeth in the security requirements. There would also be heightened fines for violations involving children under age 16.

Notably, and also similar to the GDPR, a new data protection agency would be created to take off some of the enforcement load from the Attorney General. In addition to enforcing the CCPA and the CPRA, the agency would be authorized to prepare rules and regulations. The agency would be able to issue subpoenas and would have audit powers, as well as rights to impose regulatory fines.

Given today's pro-privacy environment (especially in California), as businesses continue to navigate the CCPA, they would be well served to also consider the CPRA with an eye toward the not-too-distant future.