

1-18-2022

California Consumer Protection Act (CCPA): Narrowing CCPA Exemptions Will Ensure Greater Privacy Protections

Brennan Gamwell

Follow this and additional works at: https://digitalcommons.law.ggu.edu/ggu_law_review_blog



Part of the [Consumer Protection Law Commons](#)

GGU Law Review Blog

🕒 JANUARY 18, 2022 💬 NO COMMENTS

California Consumer Protection Act (CCPA): Narrowing CCPA Exemptions Will Ensure Greater Privacy Protections

CCPA should narrow or eliminate its long list of exempted organizations, which includes many small and medium-sized businesses, non-profits, universities, government agencies, and health institutions.



Photo by [Towfiq barbhuiya](#) on [Unsplash](#)

The **California Consumer Privacy Act (CCPA)** has been touted as a “**landmark**” and one of the “**strictest digital privacy laws in the United States.**” **Californians for Consumer Privacy** first sponsored the CCPA in 2018 as a ballot initiative. Soon after, the CCPA was introduced into the California Assembly as **AB 375** and signed into law later that same year. The CCPA went into effect on January 1, 2020, granting California residents rights regarding their personal information collected and sold by businesses.

Privacy protections for California consumers will become even stronger once the California Privacy Rights Act (CPRA) goes into effect on January 1, 2023. The CPRA is an amendment to the CCPA that will expand the definition “businesses” subject to the law and introduce a new classification of protectable, personal information, among other changes.

In spite of being hailed as a “landmark” and for its “strict” protections, CCPA’s limitations render it far less protective of individuals’ privacy and therefore dramatically less effective than its European counterpart, the **General Data Protection Regulation (GDPR)**. Notably, rights granted under CCPA apply only to *consumers* against *businesses*, a narrow band of for-profit entities that excludes many small and medium-sized businesses, non-profits, universities, government agencies, and health institutions. Unlike CCPA, the General Data Protection Regulation applies *generally*, as the name suggests, which includes the very types of entities excluded by the CCPA.

The **CCPA** applies narrowly to for-profit businesses that do business in California and meet any of the following criteria:

- “Have a gross annual revenue of over \$25 million;
- Buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices; or
- Derive 50 percent or more of their annual revenue from selling California residents’ personal information.”

CPRA will do little to expand CCPA’s applicability. In fact, CPRA may result in having the opposite effect. After CPRA’s amendments go into effect, only businesses buying, selling, receiving, or sharing more than 100,000 residents’ information will be subject to the Act, up from 50,000 under CCPA. In short, a business will need to serve double the number of California residents for the CCPA to apply.

California’s limitations on data privacy protections extend beyond those found in the CCPA. For example, **California’s data breach reporting statute** requires disclosure by only state agencies and businesses, similarly excluding organizations like non-profits and universities, that also handle large volumes of “sensitive personal information,” such as usernames, passwords, credit card information, social security numbers, etc.



Photo by [AbsolutVision](#) on [Unsplash](#).

CCPA's Expansive Exemptions Leave California Residents At Risk

According to the [California Attorney General's website](#), the CCPA grants consumers a number of rights regarding how *businesses* use and sell their information, such as the [right to know](#) about what information is collected, and how it is used and shared; the [right to delete](#) this information; the [right to opt-out](#) of the sale of this information; and the [right to non-discrimination](#) for exercising any rights under the CCPA.

CCPA's privacy protections remain illusory while expansive exemptions to compliance remain. Therefore, the California legislature should eliminate *all* exemptions from the state's privacy statute. Here is an example of how current CCPA exemptions could directly harm individuals who donate to a large nonprofit organization. Under current law, a large, California-based nonprofit would have no duty to adhere to any of the rights listed above. Likewise, such a nonprofit has no duty to disclose the impact of any data breach. Imagine if such a nonprofit did not update the default password on their [customer relationship management](#) (CRM) system, neglected to enable [multi-factor authentication](#), and as a result was subject to a large-scale data breach, exposing donors' usernames, passwords, home addresses, and credit card information—all "[sensitive personal information](#)" under CCPA. The CCPA's amendments to the CCPA require that businesses implement "[reasonable security procedures and practices](#)" to protect consumers' data. Although implementing reasonable security procedures and practices may be a best practice for any organization, this nonprofit would have no independent duty to do so. Further, the nonprofit would have no duty to report neither the breach itself, nor the details of the breach, to its patrons or to the state, unlike for-profit businesses and state agencies. Nonprofits in particular are likely to possess other categories of sensitive,

personal information, such as data on religion and sexual orientation. Despite this, [California's Office of the Attorney General](#) indicates that nonprofits are exempted from CCPA requirements.

Arguments may arise that CCPA compliance would prove onerous for organizations with limited resources. On the contrary, many organizations, including nonprofits and small businesses, rely on "service providers," like [Salesforce](#) to manage customer lists and [MailChimp](#) to manage email campaigns, that are independently subject to CCPA and provide out-of-the-box CCPA (and, in many cases, GDPR) compliance tools. Further, the CPRA has created the [California Privacy Enforcement Agency \(CPEA\)](#), which "is vested with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act." The CPEA should implement and promulgate privacy compliance guidance, training, and other resources applicable specifically to small businesses and nonprofits. The CPEA should expand enforcement activities to include these organizations as well. Enforcement could take the form of required data privacy training and ongoing audits.

In addition, eliminating exemptions from CCPA and other privacy-related statutes would reduce confusion regarding to whom CCPA applies. Businesses would no longer need to track and project their number of users or annual revenue to determine when CCPA would apply to them. Nonprofits would know exactly what privacy protections would be expected of them in order to adhere to California's privacy laws. Most importantly, California residents would enjoy comprehensive data privacy protections, rather than a short list of protections diluted by an expansive list of exemptions. Until these exemptions are eliminated and CCPA compliance is expanded, large swathes of Californians' sensitive personal information remain unprotected.

Brennan Gamwell

Brennan Gamwell is a 2022 JD candidate at the Golden Gate University School of Law in San Francisco.



Leave a Reply

Enter your comment here...

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)

Search blog

Search



Archive

Select Month



© GOLDEN GATE UNIVERSITY LAW REVIEW