By Stuart L. Pardau

Stuart L. Pardau (stuart@pardaulaw.com) is Associate Professor of Business Law, Professional Practice, in the Miami Herbert Business School at the University of Miami.

Stuart L. Pardau

In November 2020, California voters, pursuant to the ballot initiative process mandated by that state's constitution, passed another major piece of privacy legislation, the California Privacy Rights Act (CPRA), significantly expanding and updating existing privacy law under the California Consumer Privacy Act (CCPA). The new law goes into effect on January 1, 2023. In addition to the statutory provisions in CPRA, the CCPA is expected to issue supplementary regulations by July 1, 2022.

While the CCPA was the most significant development in US privacy law in years, the CPRA is arguably even more significant. Among other things, the CPRA creates a new state privacy agency, the California Privacy Protection Agency, tasked with enforcing the CPRA. The California Privacy Protection Agency is allotted an annual budget of $10 million with express authorization in the statute for the legislature to increase this budget.

Furthermore, the CPRA removes the 30-day cure period that was in place under CCPA for alleged substantive violations (for example, failure to have appropriate privacy policy provisions or other notices, or failure to properly handle consumer requests). For the party alleged of a violation, having this cure period established a safe harbor of sorts; one could be a violator but not really suffer any meaningful consequence provided the said problem was fixed within the specified time period (i.e., 30 days). Therefore, removal of this cure period is a game changer. While there was already substantial risk of litigation related to data breaches under CCPA, after CPRA, companies can add to that the risk of investigation by a well-funded state agency with the power to levy fines with no opportunity to cure.

This document is only available to members. Please log in or become a member.

Become a Member Login