

Class Action Suits Attempt To Stretch Consumers' Ability To Sue For CCPA Violations

- The CCPA's private right of action is limited. It covers consumers' right to reasonable protection against certain types of data breaches, but not the new and expansive "Privacy Rights" the act is best known for.
- Several private plaintiffs have filed putative class actions alleging CCPA violations. Some of their claims defy the act's explicit limitations by seeking redress for alleged violations of Privacy Rights.
- If courts permit these claims to move forward, it would represent a dramatic expansion of the CCPA, forcing businesses to re-assess the scope of their legal exposure.

The CCPA's Private Right Of Action

The CCPA gives consumers several new "Privacy Rights"—such as the right to know how their personal information is collected, used and shared, the right to request deletion of their personal information, and the right to opt-out of "sales" of their personal information. But the act doesn't give consumers the right to sue for a violation of Privacy Rights. The private right of action is limited to the "Security Right," which is only violated if sensitive categories of personal information are "subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices."¹ If consumers prove such a violation, the court may award (i) statutory damages up to \$750 per consumer per incident, or actual damages, whichever is greater, (ii) injunctive or declaratory relief, and (iii) any other relief the court deems proper.²

A plaintiff faces at least four major hurdles. First, the plaintiff must show an actionable data breach, which requires both "unauthorized access" **and** "exfiltration, theft, or disclosure" of the plaintiff's personal information. Second, the plaintiff must show that

the breach compromised specific types of personal information. The private right of action, set forth in Civil Code § 1798.150(a), incorporates a definition of "personal information" that is much narrower than the expansive definition used throughout the rest of the act.³ As a result, only certain types of personal information (e.g., social security numbers, driver's license numbers, payment card information, medical information, biometric data) can form the basis for a consumer lawsuit.⁴ Third, the plaintiff must show that the business failed to use "reasonable security procedures and practices." Fourth, the plaintiff must show that the business's failure to use reasonable security measures was the proximate cause of the breach.

In addition to limiting the private right of action to data breaches as defined in section 1798.150(a), the CCPA provides that a consumer action "shall not be based on violations of any other section of [the act]," explicitly barring causes of action for violation of Privacy Rights under the CCPA.⁵ On top of that, the CCPA bars plaintiffs from using an alleged CCPA violation as the basis for a cause of action under another statute: "The cause of action established by

¹ Cal. Civ. Code § 1798.150(a)(1).

² Cal. Civ. Code § 1798.150(a)(1)(A), (B), (C).

³ Compare Cal. Civ. Code § 1798.81.5(d)(1)(A), with Cal. Civ. Code § 140(o)(1).

⁴ Cal. Civ. Code § 1798.81.5(d)(1)(A).

⁵ Cal. Civ. Code § 1798.150(c).

this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title [i.e., the CCPA]. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law.”⁶

These plain limitations on the CCPA’s private right of action are supported by the Legislature’s deliberate rejection of the Senate’s proposal in May 2019 to expand the private right of action to cover all CCPA violations. The CCPA delegates enforcement of Privacy Rights exclusively to the Attorney General, who is authorized to begin enforcement action on July 1 of this year.⁷

Plaintiffs Defy The CCPA’s Express Limitations

Within the four months following the CCPA’s effective date, at least six putative class actions have been filed in California’s U.S. district courts alleging some violation of the act.⁸ Some of these plaintiffs allege a cause of action under the CCPA for violation of the Security Right. Despite the CCPA’s explicit limitations on the right to sue, some plaintiffs seek redress for alleged violations of their Privacy Rights.

Even though the CCPA expressly bars use of the act “as the basis for a private right of action under any other law,” some of these plaintiffs have alleged CCPA violations to support a cause of action under California’s unfair competition law (UCL).⁹ This generally involves alleging the purported CCPA violations, including violations of consumers’ Privacy Rights, as the underlying “unlawful, unfair, or fraudulent” business practice prohibited by the UCL. For example, the unlawful and unfair business practices alleged in support of the UCL claim against Clearview AI Inc. (“Clearview”) include purported violations of Privacy Rights under the CCPA, such as failing to provide adequate disclosures to consumers before collecting their personal information.

Other plaintiffs defy the CCPA’s express limitations even more overtly, alleging a direct cause of action under the CCPA for purported violations of Privacy Rights. For example, Zoom Video Communications, Inc. (“Zoom”) was sued under the CCPA for allegedly failing to disclose that it shared its users’ personal information with third parties, like Facebook.

Implications for Businesses

Defendants in these cases will likely move to dismiss these claims in whole or in part, based on the CCPA’s explicit limitations on the private right of action and precedents governing application of the UCL. The plaintiffs would face an uphill battle on both fronts. But if one or more of these claims survives a motion to dismiss, it could set a troubling precedent for businesses. For example, a court’s refusal to dismiss these types of claims at the pleadings stage could expose a broad swath of businesses to consumer lawsuits for allegedly making false or misleading statements in privacy policies, failing to declare “sales” of personal information and offer consumers the ability to opt-out, or violating other expansive Privacy Rights established by the CCPA. That type of exposure represents a much broader risk than potential consumer litigation limited to particular types of data breaches.

Our Privacy & Data Security team will continue to monitor these and other efforts to enforce the CCPA and provide further updates.

Authors:

Travis P. Brennan
949.725.4271
tbrennan@sycr.com

Mayant Luk
949.725.4057
mluk@sycr.com

⁶ Id.

⁷ Cal. Civ. Code § 1798.155(b).

⁸ *Lopez v. Tandem Diabetes Care, Inc.*, Case No. 3:20-cv-00723 (S.D. Cal.), filed April 16, 2020; *Cullen v. Zoom Video Communications, Inc.*, Case No. 5:20-cv-02155 (N.D. Cal.), filed March 30, 2020; *Fuentes v. Sunshine Behavioral Health Group, LLC*, Case No. 8:20-cv-00487 (C.D. Cal.), filed March 10, 2020; *Burke v. Clearview AI, Inc.*, Case No. 3:20-cv-00370 (S.D. Cal.), filed Feb. 27, 2020; *Sheth v. Ring LLC*, Case No. 2:20-cv-01538 (C.D. Cal.), filed Feb. 18, 2020; *Barnes v. Hanna Andersson LLC*, Case No. 4:20-cv-00812 (N.D. Cal.), filed Feb. 3, 2020.

⁹ Cal. Civ. Code § 1798.150(c).