

Calif. Privacy Law Will Likely Prompt Flood Of Class Actions

By Alexis Buese

Law360 (May 15, 2019, 11:41 AM EDT) -- The California Consumer Privacy Act, known as the CCPA, is a new law set to go into effect on Jan. 1, 2020. The CCPA is the first U.S. law that will require businesses with an online presence in California to focus on user data and it regulates how businesses collect, share and use such data. One of the most significant risks to online business providers in California is that the CCPA provides for a private right of action for California consumers.

As currently drafted, the private right of action is limited to instances in which a consumer's nonencrypted or nonredacted personal information is subject to unauthorized access and exfiltration, theft or disclosure as a result of a business's failure to maintain reasonable security procedures. In April, California legislators voted on several amendments to the CCPA, one of which sought to expand the private right of action against entities that violate the CCPA to any violation of the CCPA.

The amendment, while approved unanimously, was placed in the suspense file, where bills with significant fiscal impacts are held so that the California Senate Appropriations Committee can evaluate the total budgetary impact. The deadline for the committee to report bills to the Senate floor from the suspense file is May 17. If the amendment survives the suspense procedure, it will go to the Senate floor for a vote. If it passes the Senate, then the bill will move on to the Assembly.

Regardless of the ultimate fate of the amendment, businesses should still be wary. While most of the focus on the CCPA has been on preparing for the enactment of the CCPA, this article focuses on consumer class action litigation exposure. Given the unprecedented change to California law, the CCPA will invite an explosion of consumer litigation as plaintiffs seek to recover statutory damages under the private right of action and the California Unfair Competition Law, or UCL.[1] As e-commerce businesses continue to develop new and innovative ways to sell their goods and services to customers in California, they must remain vigilant in preparing for the likely tide of litigation that will stem from the enactment of the CCPA.

The Private Right of Action as a Predicate for Consumer Class Action Litigation

The CCPA allows consumers, to bring lawsuits when their "nonencrypted or nonredacted personal information ... is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information." Significantly, the CCPA provides consumers with the ability to seek either actual damages or statutory damages up to \$750 per incident.

In determining the proper amount of statutory damages, courts are obligated to consider, among other elements, "the nature, seriousness ... and persistence of the misconduct," number of violations, "the length of time over which the misconduct occurred," willfulness, and ability to pay. Further, the court may order injunctive or declaratory relief, or any other relief deemed proper for violations of this provision.

The private right of action is available only if it involves unauthorized access to the data and also results from unreasonable security. But, significantly, "reasonable" security measures are not defined by the CCPA, nor has California codified what is meant by "reasonable security." In the absence of a concrete definition, current best practices would suggest ensuring security policies and practices adhere to recognized security frameworks. Ultimately, however, the boundaries of what is or is not reasonable will likely have to be determined by a court.

Furthermore, the right to statutory penalties did not previously exist for data breaches involving California residents' personal information. The fact that statutory damages are now available is expected to provide incentive for plaintiffs to bring class action litigation. Indeed, in the typical class action data breach litigation, the question of standing has been paramount.

Plaintiffs have often struggled to sufficiently demonstrate that a theft of their data resulted in an injury in fact. The new allowance for statutory damages has cleared a major litigation hurdle for plaintiffs as they will no longer need to demonstrate that an actual financial injury has been suffered. With a statutory damages award of up to \$750 per violation, the CCPA creates a possibility for staggering verdicts in the consumer class action context.

A California resident may only initiate a lawsuit after giving businesses' notice and a 30-day opportunity to cure. If the business cures the violation and provides the consumer with an "express written statement that the violations have been cured and that no further violations shall occur," the consumer cannot initiate an action. As drafted, the safe harbor provision is a double-edged sword.

On the one hand, the safe harbor provision will provide businesses with advance notice of claims and the ability to engage plaintiffs before litigation progresses. On the other hand, because of the uncertainty in the statute as drafted, it is not clear what an actual cure of the data breach would look like. Questions abound, including how to cure a security breach that has already occurred. This cure period is similar to the notice and cure period under the California Consumers Legal Remedies Act, or CLRA, in which the plaintiffs bar is well versed at requesting "cures" that may be difficult to achieve. E-commerce businesses can expect to grapple with the question of whether a cure was adequately provided in a CCPA class action lawsuit.

California Consumer Laws as a Predicate for Consumer Class Action Litigation

The CCPA may spark expanded class action litigation as plaintiffs attorneys use existing California consumer laws to enable lawsuits for CCPA violations beyond the data breach provision. The unfair competition law permits any person, acting for the interests of itself, its members or the general public, to initiate an action for restitution or injunctive relief against a person or business entity who has engaged in "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising."

The UCL is a powerful tool for plaintiffs who use its extensive equitable remedies and far-reaching liability standard to pursue consumer class action claims. Consequently, plaintiffs lawyers are likely to use the CCPA to advance two principal arguments.

First, plaintiffs counsel will likely argue that if there has been a violation of the data breach provision, then plaintiffs may pursue "unlawful" claims for data breaches. While the CCPA expressly provides that, "[n]othing in this act shall be interpreted to serve as the basis for a private right of action under any other law," the boundaries of this limitation are likely to be tested in litigation.

Litigants will likely argue that there is sufficient California case law that permits consumers to base UCL violations on laws that do not explicitly provide a private right of action. Second, the plaintiffs bar will likely pursue violations of the CCPA not related to data breaches to advance secondary UCL claims. E-commerce businesses can expect to see arguments that the limiting clause in the CCPA only applies to the data breach claims.

Defendants can advance arguments that the language of the CCPA should be read to broadly bar private suits based on violations of the law since the California attorney general is ultimately vested with that authority. While much remains to be seen, courts will likely be focused on whether the legislature specifically intended to preclude UCL claims.

Consider Ways to Reduce Litigation Exposure

In addition to instituting CCPA compliance and preparedness in order to comply with the CCPA's notice and disclosure obligations, companies should consider including an arbitration clause and a class action waiver in the website's terms and conditions, prohibiting users from litigating en masse. While the CCPA includes a prohibition on contract terms that appear targeted at arbitration clauses and class action waivers, this should be preempted by the Federal Arbitration Act, or FAA.

In recent decisions like *AT&T Mobility LLC v. Concepcion*,^[2] and *DirecTV Inc. v. Imburgia*,^[3] the [U.S. Supreme Court](#) confirmed that class actions waivers in arbitration provisions are enforceable. In 2017 the Supreme Court in *Kindred Nursing Centers L.P. v. Clark*^[4] reaffirmed that the FAA preempts state laws placing agreements to arbitrate on weaker footing than other types of contract. The Supreme Court found that a state court rule was really an attempt to target and disfavor arbitration agreements, and, on that basis, held the arbitration agreement at issue was to be enforced. Based upon the recent Supreme Court decisions vacating anti-arbitration state rules, it seems likely the attempt by the CCPA to prevent arbitration and class action waivers will be preempted.

Businesses also should critically analyze the conspicuity of their websites' notices of the terms and conditions, the accessibility and the timing of the notices, as well as the notice and placement of the arbitration provision itself. The terms and conditions must be presented in a manner that provides adequate notice to the user, focusing on the design and content of the website, and terms and conditions page. To maximize the likelihood of enforcement, the terms should be clear and conspicuous, easily accessible and displayed in a sufficiently large viewing window to provide the user an adequate opportunity to review the terms, thereby eliminating any doubts that a reasonable user would have noticed them. Courts have been more willing to enforce terms and conditions communicated through "clickwrap" agreements that require the user to affirmatively accept the contractual terms before proceeding to the next step in the transaction.

To maximize enforceability when including an arbitration clause, e-commerce businesses should also consider including a delegation clause to the arbitrator. On Jan. 8, 2019, the U.S. Supreme Court issued its decision in *Henry Schein Inc. v. Archer and White Sales Inc.*,^[5] holding that a court may not override the contractual agreement that delegates arbitrability questions to the arbitrator and rejected the "wholly groundless" exception to the contractual delegation of arbitrability questions. Schein gives online businesses an even greater ability to limit courtroom litigation, and businesses should consider vesting an arbitrator with the power to decide both substantive and threshold questions affecting the parties' rights to litigate.

The placement of the arbitration provision is also essential to providing the user notice in order to form a binding arbitration agreement. The terms and conditions can ensure sufficient notice of the arbitration agreement by:

- Including a statement up front that the terms and conditions contain a binding arbitration clause
- Stating unequivocally that the parties have agreed to binding arbitration.
- Explaining how an arbitration proceeding can be commenced.
- Providing users an opportunity to opt out of the arbitration agreement and informing them that by not doing so, they are agreeing to the arbitration clause.

Finally, in addition to presenting the arbitration provision in a manner that provides adequate notice to the user, businesses should evaluate whether their arbitration provision includes easily understandable, balanced provisions to avoid a finding of unconscionability.

Concluding Thoughts

The CCPA has potentially far-reaching implications for class action litigation and will not go unnoticed by the plaintiffs bar when it goes into effect Jan. 1, 2020. Practitioners should anticipate class action litigation issues early, and be aware of the preventative measures that can be taken by businesses, including the implementation of privacy and data policies and effective terms and conditions, to minimize the potential

for significant exposure.

[Alexis Buese](#) is a partner at [Sidley Austin LLP](#).

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] (Cal. Bus. & Prof. Code § 17200).

[2] [AT&T Mobility LLC v. Concepcion](#), 563 U.S. 333 (2011)

[3] [DirecTV Inc. v. Imburgia](#), 136 S. Ct. 463 (2015)

[4] [Kindred Nursing Centers L.P. v. Clark](#), 137 S.Ct. 1421 (2017)

[5] [Henry Schein, Inc. v. Archer and White Sales, Inc.](#), No. 17-1272

Article Link: <https://www.law360.com/articles/1159313/calif-privacy-law-will-likely-prompt-flood-of-class-actions>