Lessons From 6 Months Of Calif. Privacy Law Litigation

By **Natasha Kohne, Michelle Reed and Molly Whitman** (July 10, 2020)

Natasha Kohne

Michelle Reed

Molly Whitman

It has been two years since the California Consumer Privacy Act was signed into law on June 28, 2018, creating an expansive framework to govern the collection, usage, disclosure and security of California residents' personal information.

Although the CCPA went into effect on Jan. 1, the California attorney general submitted the final draft of proposed regulations to the California Office of Administrative Law just last month.[1]

CCPA's Private Right of Action

Plaintiffs have long sought recompense for data breaches, often alleging negligence, breach of contract, violation of breach notification statutes, and violation of state unfair trade practice statutes, yet plaintiffs struggled to establish standing or to allege a cognizable injury under these causes of action without particularized allegations of actual loss or damage due to the breach, e.g., identity theft.[2]

Recognizing these limitations, the CCPA specifically includes a limited private right of action for California residents to seek actual or statutory damages if certain statutorily defined personal information has been "subject to an unauthorized access and exfiltration, theft or disclosure" due to a business's failure to "implement and maintain reasonable security procedures."[3]

As a result, businesses that suffer data security breaches must now contend with additional class action exposure from California consumers whose data may have been disclosed in the breach.

Many have speculated that because the CCPA provides statutory damages for each incident, without articulating a requirement to prove actual harm, the CCPA will elicit more class actions.[4] While the statutory damages are limited to between $100 and $750 per consumer per incident, the potential exposure for businesses may be astronomical when damages are compounded by the number of California-based consumers alleging their data was compromised.[5]

CCPA Litigation Trends

The attorney general's enforcement authority went into effect on July 1, so the second half of 2020 will reveal much about the attorney general's enforcement strategy. The strategy of private litigants, who have been able to file CCPA claims since Jan. 1, may be instructive on what to expect for enforcement.[6]

Despite court closures and general business disruption caused by the COVID-19 pandemic, the delayed legal environment has not stymied the filing of complaints bringing either direct CCPA claims or referencing the CCPA within a separate cause of action.

In fact, the rapid migration to remote work has spawned several CCPA actions, as threat

actors have exploited the transitional chaos and strain on information technology departments dealing with a large population of workers who are working from home — many from personal computers — for the first time.

Thus far, April has been the most active month for new CCPA cases, with over a dozen complaints being filed in both state and federal courts. As many of the defendant businesses are incorporated in other states, it is unsurprising that most cases have been filed in federal court.

Additionally, since the CCPA only governs the privacy rights of California residents, it is likewise unsurprising that California is the predominant venue, though some cases have also popped up in federal courts in Florida, New York and Washington, for instance.

The CCPA has yet to be interpreted in court. Below, we discuss some of the plaintiffs' pleading strategies that will be tested in the coming months.

Cases That Exceed the Boundaries of the Limited Private Right of Action

The limitations on the CCPA's private right of action are clear. Section 1798.150(a)(1) states:

> Any [California resident] consumer whose nonencrypted and nonredacted personal information ... is 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 appropriate to the nature of the information to protect the personal information may institute a civil action.

Civil actions maybe be instituted for actual or statutory damages, injunctive relief and other relief the court deems proper.

Thus, the civil private right of action applies only if personal information has been the subject of a data breach and the statute makes clear that the "cause of action established by 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."[7]

California Attorney General Xavier Becerra underscored this point in a June 30 press release, stating:

> The CCPA gives consumers a limited right to sue a business for a data breach that was a result of a business's failure to reasonably secure certain types of personal information. It does not give consumers the right to sue businesses for other violations of the CCPA.[8]

Nevertheless, it was anticipated that plaintiffs would experiment and push the boundaries by filing civil actions that allege violations of CCPA provisions other than Section 1798.150, and the case statistics to date show this to be true.

For example, with the rise of videoconferencing due to COVID-19, multiple class actions have been filed against Zoom Video Communications Inc.

Outside of Section 1798.150, these putative class action complaints also include claims based on "collecting and using personal information without providing consumers with adequate notice consistent with the CCPA, in violation of Civil Code Section

1798.100(b),"[9] and for failing to notify consumers of their right to opt-out of the disclosure of their personal information to third parties pursuant to Section 1798.120(b).[10] None of the allegations relate to the limited private right of action of a data breach provided for under the CCPA.

While it does not appear from a plain reading of the statute that consumer claims for violations outside of Section 1798.150 will survive the pleadings stage, these claims underscore plaintiffs' tenacity in seeking a potential foothold to recuperate statutory damages even if they cannot show that their data was actually compromised in a breach.

Cases That Use the CCPA to Bolster Other Causes of Action

Since some provisions of the CCPA have a 12-month look-back period, but the private right of action provision does not, some commentators have opined that consumers may only file civil actions related to breach events that occurred on or after Jan. 1.[11] Perhaps to skirt this limitation, some complaints allege CCPA violations while not actually pleading a CCPA cause of action.

For example, in Barnes v. Hanna Andersson LLC, the plaintiffs alleged that their personal information was exposed during a September 2019 data breach.[12] Though the complaint alleges the putative class members may have suffered deprivation of rights they possess under the CCPA, the only causes of action alleged are negligence, declaratory judgment and violation of the California Unfair Competition Law.

On June 3, however, the plaintiffs amended their complaint to include a CCPA cause of action.[13] It remains to be seen how courts will apply this statute to breach events that occurred prior to the CCPA's effective date.

Other plaintiffs have taken a different track, perhaps acknowledging that the private right of action is not retroactive. In a recent case against Plaid Inc. the plaintiff alleged that Plaid violated several statutes by creating the "greatest database of consumer transactional data in history" and failing to inform consumers of that collection in its privacy notice.[14] The plaintiff did not allege a CCPA cause of action, but alleged that Plaid engaged in an unlawful business practice under the UCL by violating the CCPA as a predicate act.[15]

No court has yet reached the question of whether a CCPA violation may support a UCL claim. Plaintiffs argue that almost any law — federal, state or local — can serve as a predicate for a UCL claim, but courts have made clear that no private cause of action exists if the predicate statute expressly bars enforcement under the UCL.[16]

The CCPA expressly precludes consumers from using it as "the basis for a private right of action under any other law," which evinces the legislature's intent to bar the CCPA from supporting other statutes as a predicate act.[17] This is further bolstered by Section 1798.155, which endows the attorney general with broad enforcement authority over all CCPA violations, thereby obviating the need for enforcement via any other consumer protection vehicle.[18]

Looking Ahead

The CCPA's first six months have produced more than 50 consumer class actions alleging some form of a CCPA violation, and there is no sign of slowing down in the second half of 2020.

As the attorney general's enforcement powers just went into effect, we expect the next six months to see a flurry of continued activity in both consumer class actions and state enforcement.

Importantly, even though the CCPA regulations are not yet effective, it appears that the attorney general may bring enforcement actions for CCPA violations that occurred any time after Jan. 1, relying on the statute rather than the implementing regulations.[19] Thus, a business that has already been hit with a consumer class action may be subject to an upcoming enforcement action as well.

Although businesses were given lead time to become CCPA compliant prior to Jan. 1, many feared the statute's onerous requirements for companies that collect, process or sell large amounts of consumer data. Coupled with a new age of telework and the heightened possibility of business email compromises and other data security breaches, the liability risk for failing to comply with the CCPA is significant.

Moreover, the California Privacy Rights Act has recently qualified for the November 2020 ballot. If enacted, the CPRA — or CCPA 2.0 — will enhance California consumers' data privacy rights and permit even more control over their data. Notably, the CPRA would create a new agency to address privacy issues, including enforcing the CCPA. Having an agency devoted solely to enforcing consumer privacy rights would likely increase the number of CCPA enforcement actions being filed.

As the whirlwind first half of 2020 comes to a close, companies should be vigilant in CCPA compliance in order to avoid becoming the next target of CCPA enforcement.

Natasha G. Kohne and Michelle A. Reed are partners, and Molly E. Whitman is counsel, at Akin Gump Strauss Hauer & Feld LLP.

[1] See Office of the Attorney General of the State of California, California Consumer Privacy Act Regulations: Information About the Rulemaking Process, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-rulemaking-fact-sheet.pdf. Once approved by the OAL, the final regulation text will be filed with the Secretary of State.

[2] See, e.g., Krottner v. Starbucks Corp., 406 Fed. App'x 129 (9th Cir. 2010) (allegation of future identity theft was not a cognizable injury for purposes of negligence claim); In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 963 (S.D. Cal. 2012) (dismissing claims under consumer protection statutes because allegations that "the heightened risk of identity theft, [and] time and money spent on mitigation of that risk" were insufficient to establish standing).

[3] Cal. Civ. Code § 1798.150(a).

[4] Id. § 1798.150(a)(1).

[5] Id.

[6] Id. § 1798.185(c).

[7] Id. § 1798.150.

[8] Press Release, Office of the Attorney General of the State of California, Attorney General Becerra Reminds Consumers of Data Privacy Rights Under the California Consumer Privacy Act (June 30, 2020), https://oag.ca.gov/news/press-releases/attorney-general-becerra-reminds-consumers-data-privacy-rights-under-california.

[9] Cullen v. Zoom Video Commc'ns, Inc., No. 5:20-cv-02155-SVK, ECF No. 1 at ¶ 33 (N.D. Cal. Mar. 30, 2020).

[10] See Taylor v. Zoom Video Commc'ns, Inc., No. 5:20-cv-02170, ECF No. 1 at ¶ 132 (N.D. Cal. Mar. 31, 2020). See also Ohlweiler v. Zoom Video Commc'ns, Inc., No. 2:20-cv-03165 (C.D. Cal. Apr. 3, 2020); Jimenez v. Zoom Video Commc'ns, Inc., No. 5:20-cv-02591 (N.D. Cal. Apr. 14, 2020); Henry v. Zoom Video Commc'ns, Inc., No. 5:20-cv-02691 (N.D. Cal. Apr. 17, 2020).

[11] See, e.g., Cal. Civ. Code § 1798.130.

[12] Barnes v. Hanna Andersson, LLC, No. 3:20-cv-00812-EMC, ECF No. 2 (N.D. Cal. Feb. 3, 2020).

[13] Id.; Barnes v. Hanna Andersson, LLC, No. 3:20-cv-00812-EMC, ECF No. 46 (N.D. Cal. June 3, 2020).

[14] Mitchell v. Plaid, Inc., No. 3:20-cv-04230, ECF No. 1 at ¶ 7 (N.D. Cal. June 25, 2020).

[15] Id. at ¶ 196.

[16] See Rannis v. Fair Credit Lawyers, Inc., 489 F. Supp. 2d 1110, 1119 (C.D. Cal. 2007), aff'd sub nom. Rannis v. Recchia, 380 Fed. App'x 646 (9th Cir. 2010) (citing Stevens v. Sup. Ct., 602, 89 Cal. Rptr. 2d 370 (Cal. App. 4th 1999)); Cal. Bus. & Prof. Code § 17200.

[17] Cal. Civ. Code § 1798.150(c).

[18] Id. § 1798.155.

[19] The regulations were submitted to the OAL on June 1, 2020, and the OAL has 30 working days plus 60 calendar days to determine whether the regulations satisfy the procedural requirements of the Administrative Procedure Act. Even though the regulations have not yet been approved by OAL, the CCPA allows enforcement of the statute itself on July 1, 2020. See Cal. Civ. Code § 1798.85(c).