

[Blogs](#)

April 02, 2020

CCPA in Litigation: 2018 to Present

The California Consumer Privacy Act (CCPA) went into effect three months ago, on January 1, 2020. Although enforcement by the California attorney general cannot begin until July 1, private plaintiffs have been able to bring claims under the law's limited private right of action since the beginning of the year. The CCPA is already having an impact on litigation. Two high-profile cases filed after January 1 directly allege violations of the CCPA and have attracted attention. Other cases that either allege CCPA violations or otherwise cite to the statute have received less notice. Even if the cases do not result in decisions that are binding on future litigants, the arguments are worth a look because they may signal trends for which privacy litigators should be prepared. To that end, this privacy quick tip aims to paint a broader picture of how the CCPA has been referenced in litigation and identify a few potential trends to keep an eye on.

Cases Alleging CCPA Violations

To date, at least 13 cases have alleged violations of the CCPA. Of those, at least nine are class actions, four were brought by pro se litigants, and five were filed before the CCPA went into effect. In the class action lawsuits, some of the CCPA claims were brought squarely under the statute's limited private right of action (Cal. Civ. Code § 1798.150), but several of the other claims are less direct and test the limits of section 1798.150. For example, some claims rely on an alleged violation of the CCPA to support a violation of another law (although this approach appears to be prohibited by section 1798.150(c)). Other claims purport to allege a violation of other provisions of the CCPA, without reference to the limited private right of action in section 1798.150.

Claims Brought Under the Private Right of Action The CCPA provides only a very limited private right of action. A consumer can bring a private suit against a business under CCPA section 1798.150(a) only if the consumer's "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." However, few class actions bring CCPA claims exclusively under section 1798.150. *See, e.g.*, Complaint, *Fuentes v. Sunshine Behavioral Health Group, LLC*, No. 8:20-cv-00487 (C.D. Cal. filed Mar. 12, 2020); *see also* Complaint, *Cullen v. Zoom Video Commc'ns, Inc.*, No. 5:20-cv-02155 SVK (N.D. Cal. filed Mar. 30, 2020) (including a 1798.150 violation among other CCPA-related claims). **Claims Not Brought Under CCPA's Limited Private Right of Action** Section 1798.150(c) of the CCPA clarifies that "[t]he cause of action established by [section 1798.150] . . . shall not be based on violations of any other section of this title."

Nonetheless, at least four class action cases (in addition to a few pro se cases) have included alleged violations of the CCPA that are not premised on section 1798.150. *See, e.g.*, Complaint, *Cullen*, No. 5:20-cv-02155 SVK (alleging violation of the CCPA's notice requirements under 1798.100(b) in addition to a violation under section 1798.150(a)); Complaint at 5, *Hernandez v. PIH Health, Inc.*, No. 2:20-cv-1662 (C.D. Cal. filed Feb. 20, 2020) (class action based on a data breach, but alleging with respect to the CCPA claim "deprivation of rights possessed under . . . California Consumer Privacy Act"). **CCPA as the Basis for Other Violations of Law** Section 1798.150(c) of the CCPA states: "Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law." Despite this, at least three class action lawsuits rely on alleged violations of the CCPA to support claims under the California Unfair Competition Law (UCL) (codified at Cal. Bus & Prof. Code §§ 17200 et seq.). *See* Complaint, *Cullen*, No. 5:20-cv-02155 SVK; Complaint, *Burke v. Clearview AI, Inc.*, No. 3:20-cv-00370 BAS MSB (S.D. Cal. filed Feb. 27, 2020); Complaint, *Almeida v. Slickwraps Inc.*, No. 2:20-cv-00559-TNL-CKD (E.D. Cal. filed Mar. 12, 2020). *See also* Complaint, *Dennis v. First Am. Title Co.*, No. 8:19-cv-01305 (C.D. Cal. filed July 1, 2019) (class action suit alluding to defendant's reference to the CCPA in its 10-K filings in support of plaintiff's UCL claim).

Litigation Otherwise Invoking CCPA

Since enactment, the CCPA has been referenced by parties (and at least one court) in more than 20 cases. Reviewing these references—a large majority of which were made in 2019 before the law went into effect—reveals a few emerging trends. **To Oppose Discovery** The CCPA has been invoked to oppose discovery. The CCPA was recently raised in an amicus brief submitted on behalf of several companies in support of a petition for certiorari to the U.S. Supreme Court. The petitioners are challenging production of information via keyword search methodology. After explaining their position that the production method is overbroad in violation of individuals' and companies' privacy interests, petitioners close the argument by citing the CCPA: "Protecting the privacy of employee data is increasingly important for amici companies and others. California recently enacted the California Consumer Privacy Act (CCPA), a sweeping privacy law The CCPA is likely only the first of many such laws to come in the United States intended to protect the personal and private data of individuals. Broad discovery orders, like the Order here, contravene the purpose of regulations like the CCPA and the growing trend of protecting privacy rights, hamper companies' compliance with statutes like the CCPA, and subject them to penalties." *Actavis Holdco U.S., Inc. v. Connecticut*, No. 19-1010, 2020 WL 1313351, at *13 (U.S. Mar. 16, 2020). Similarly, last fall in a brief filed in the U.S. District Court for the Eastern District of Wisconsin, the CCPA was discussed in support of an argument opposing a motion to compel discovery of customers' names, addresses, and phone numbers: "There were and are two main sources for this concern [that discovery might violate the privacy of customers]. First, there is the California Consumer Privacy Act of 2018 ('CCPA'), which becomes effective on January 1, 2020, with some operative provisions delayed until July 1, 2010 The main thrusts of the CCPA are to: 1. Give a consumer the right to access information about him/her held by a business; and 2. Give a consumer the right to prevent a business from selling such information—not a direct issue here." *Lehman v. Rheem Mfg. Co.*, No. 2:19-cv-00157-PP (E.D. Wis. filed Sept. 13, 2019) (footnote omitted). In a case against a large online retailer filed last July, the plaintiffs invoked the CCPA in a slightly different manner to oppose discovery. They argued that the retailer had no need to compel plaintiff to produce information because of the retailer's pending need under the CCPA to be able to produce and delete data of the type it was requesting from plaintiff. In other words, due to the retailer's obligations to respond to consumer rights requests under the CCPA, it could be presumed that the retailer was already in possession of plaintiff's personal information and therefore discovery should not be compelled. **To Broaden the Definition of Personal Information (PI)** Some parties, as in the following examples, have cited the CCPA claiming that its expansive definition of PI has some bearing on issues in dispute:

- In an amicus brief filed in the Supreme Court of Montana, petitioners cite the CCPA's definition of PI in support of what appears to be an argument that use of inferences based on PI are (or ought to be) of concern to consumers: "One reason consumers may not want a relationship with Bank of America is that [appellee] provides the bank with the names and contact information of patients owed a refund. The bank could use that information to create a detailed personal profile of the consumer when combined with other publicly and non-publicly available data. See California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.140(o)(1)(K) (defining protected 'personal information' to include 'Inferences . . . to create a profile about a consumer. . . .')." *Bratton v. Sisters of Charity of Leavenworth Health Sys.*, No. DA 19-0357, 2019 WL 6352558, at *5 (Mont. Oct. 3, 2019) (Appellate Brief).
- In appellant's opening brief before the Ninth Circuit Court of Appeals, supporting the assertion that browsing history collected via cookies is PI, appellant cited the CCPA's definition and emphasized that it includes "browsing history, search history, and information regarding a consumer's interaction with an internet website" *McGarry v. Delta Air Lines, Inc.*, No. 19-55790, 2019 WL 6329776, at *63 n.8 (9th Cir. Nov. 18, 2019) (Appellate Brief) (emphasis omitted) (quoting Cal. Civ. Code § (1798.140(o)(1)(F)).

To Support a Privacy-Related Argument Finally, another category of cases, including the following, draw upon the CCPA to attempt to support a pro-privacy argument or position:

- California Supreme Court Justice Cuéllar, in a concurring opinion in *Troester v. Starbucks Corp.*, 5 Cal. 5th 829, 837 (2018), remarks: "[W]e must be wary of any future holding that would incentivize a drastic increase in the scope and intensity of employee monitoring, which might systematically erode employees' ability to find even a moment of privacy in their lives[.]" citing to the CCPA to add that "[t]his is especially true as privacy issues have launched to the national stage and resulted in new laws in our state safeguarding privacy in our personal data, albeit in the consumer law context."
- In an amicus brief on behalf of technology companies submitted to the Ninth Circuit Court of Appeals regarding unsealing certain court proceedings, petitioners argue: "In addition to being the right thing to do, in today's marketplace, providers must build privacy and security into their offerings or risk losing customers and face Attorney General or FTC enforcement actions. . . . Against this backdrop, a company that does not take privacy and security seriously will not be able to compete effectively. This necessarily involves understanding what the government might successfully demand of it when designing its products and what design decisions carry legal consequences. . . . Privacy- and security-minded companies must, for example, understand - and account for in initial product design - whether any required redesign weakens overall security of their products, as well as any ancillary affects [sic] such redesign might have on their products." *Am. Civil Liberties Union Found. v. U.S. Dept. of Justice*, No. 19-15472, 2019 WL 2647876, at *10 (9th Cir. filed June 19, 2019) (footnotes omitted) (referencing the CCPA's private right of action).
- Plaintiffs in *Burke v. Clearview AI*, after commenting on the singular risk posed by biometric data and citing the FTC's urging of companies to ask for consent before scanning and extracting such data from photographs, claim that "[t]his prevailing view has been adopted by both the [Illinois biometric data statute] and the CCPA, which require notice to and consent from the person [whose] biometric identifier or information is being used." *Burke*, Complaint at 12.
- In *Padron v. City of Parlier*, 19CECG03894 (filed Oct. 28, 2019), the plaintiff references enactment of the CCPA for the notion that there is broad consumer support for increased regulation in California, added as general support for plaintiff's negligence claim.

The cases we've aggregated here indicate that the CCPA has impacted litigation. We will continue to track this impact, which may change course or increase as implementation of the law hits new milestones, including enforcement by the California attorney general (July 1 of this year) and finalization of the AG's draft regulations.

Authors

Explore more in

[Privacy & Security](#)