

# CCPA Litigation Round-Up

Alysa Z. Hutnik

April 7, 2020



The [California Consumer Privacy Act \(CCPA\)](#) took effect January 1, 2020. While the [California Attorney General's](#) enforcement authority is delayed until July 1, private litigants have already started to file direct claims under the CCPA as well as other consumer-related causes of actions predicated on alleged CCPA violations. Notably, the California Attorney General takes the position that enforcement actions can cover violations that predate July 1, 2020.

As detailed in our prior posts (*see, e.g.,* [here](#) and [here](#)), the CCPA expressly provides for only a limited private right of action related to data security breaches. Cal. Civ. Code 1798.150. Private plaintiffs can recover actual damages or statutory damages of \$100 to \$750 per statutory violation. While a broader potential private right of action was considered, which would have permitted individuals to sue for additional CCPA violations, that amendment (SB 561) failed.

Nevertheless, private litigants have thus far filed CCPA-related claims in cases where breaches have occurred, but also in cases where no breach is alleged. A quarter of the year in, we consider here how the CCPA has already impacted consumer class action claims.

## ***Barnes v. Hanna Andersson LLC and Salesforce.com Inc., Case No. 4:20-cv-00812 (N.D. Cal.)***

On February 3, 2020, California consumer Bernadette Barnes filed a putative class action Complaint against retailer Hanna Andersson arising from a data breach. The breach (which occurred in September-November 2019), allegedly resulted in the loss of personally identifiable information ("PII"), including unencrypted credit card and consumer information. Plaintiff also sued the cloud vendor Salesforce.com that allegedly stored the PII at issue.

Plaintiff seeks to represent a nationwide class including: "All individuals whose PII was compromised in the data breach announced by Hanna Andersson on January 15, 2020," as well as a California subclass. Plaintiff does not include a cause of action under the CCPA, but relies upon the CCPA as a predicate for her claim under California's Unfair Competition Law, Cal. Bus. & Prof. Code §17200 ("UCL"), along with causes of action for negligence and a declaratory judgment.

## ***Sheth v. Ring LLC, Case No. 2:20-cv-01538 (C.D. Cal.)***

On February 18, 2020, Seattle, Washington consumer Abhi Sheth filed a putative class action Complaint against California-based video doorbell and security camera manufacturer Ring. Plaintiff alleges inadequate security measures for handling PII as well as unauthorized disclosure to third parties.

Plaintiff seeks to represent a class of consumers defined as: “All persons residing in the United States who purchased a Ring Security Device within the applicable statute of limitations period. Plaintiff’s CCPA claim alleges improper collection and use of personal information without notice, and failing to provide the required notice of a right to opt out of the sale of personal information to third parties. Plaintiff does not allege that Ring had any specific data breach or security event that triggered the claim. Plaintiff asserts seven other causes of action arising from the same facts: invasion of privacy; negligence; breach of implied warranty of merchantability; breach of implied contract; unjust enrichment; and violations of the UCL and California Legal Remedies Act, Cal. Civ. Code § 1750, *et seq.* (“CLRA”).

Significantly, the arbitration clause in Ring’s consumer agreement may create the first opportunity to balance the CCPA’s perceived hostility to arbitration, on the one hand, and the parties’ contract and policy underlying the Federal Arbitration Act, on the other. That issue is expected to be a heavy battleground in CCPA consumer class actions, making this a potentially important first test on that issue.

On March 5, the *Sheth* case was consolidated with four other privacy-related cases pending against Ring and on March 31, the separate *Sheth* case was closed. The continuing matter, *In re: Ring LLC Privacy Litigation*, Case No. 2:19-cv-10899 (C.D. Cal.), began with a December 26, 2019 Complaint that does not reference the CCPA; however, the Court’s February 11 Consolidation Order permits the plaintiffs to file a Consolidated Complaint after interim class counsel is appointed. It is reasonable to expect that the updated pleading and addition of *Sheth* to the consolidated action could inject the CCPA more directly into the overall claims.

***Burke v. ClearviewAI, Inc., Case No. 3:20-cv-00370 (S.D. Cal.)***

On February 27, 2020, California consumer Sean Burke and Illinois consumer James Pomerene filed a putative class action Complaint against ClearviewAI (and its two founders) alleging the improper collection and sale of PII and biometric information in violation of, among other laws, the CCPA. Clearview “scrapes” websites (scanning, extracting, and copying images) to compile a comprehensive database that allegedly includes over three billion images and PII of consumers, which Clearview sells to law enforcement and private entities. Plaintiffs allege that Clearview collected and used their PII without notice or consent in violation of the CCPA.

Plaintiffs seek to represent three California-related sub-classes:

(a) Sub-Class One (the “CCPA Class”) (Cal. Civ. Code § 1798.100, *et seq.*): All persons who, while residing in California, had their California Biometric Information collected and/or used by Clearview without prior notice by Clearview and without their consent.

(b) Sub-Class Two (the “Commercial Misappropriation Class”) (Cal. Civ. Code § 3344): All persons who, while residing in California, had their Photograph or likeness knowingly used by Clearview for commercial gain without their consent.

(c) Sub-Class Three (the “Unjust Enrichment Class”): All persons who, while residing in California, had their California Biometric Information misappropriated by Clearview from which Clearview was unjustly enriched.

The Complaint also asserts claims under the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (“BIPA”) as well as specific causes of action for violations of the UCL, commercial misappropriation, and unjust enrichment.

***Cullen v. Zoom Video Communications, Inc., Case No. 5:20-cv-02155 (N.D. Cal.)***

On March 30, 2020, California consumer Robert Cullen filed a putative class action Complaint against online video-conferencing provider Zoom alleging the failure to properly safeguard user information and improper disclosure of individual and business information to third parties, including Facebook. The allegations arise from a March 26 Vice Media report that purports to detail unauthorized sharing and data vulnerabilities of Zoom.

Plaintiff seeks to represent a class comprised of: “All persons and businesses in the United States whose personal or private information was collected and/or disclosed by Zoom to a third party upon installation or opening of the Zoom video conferencing application.”

Plaintiff asserts a claim under the CCPA for Zoom’s alleged collection and use of PII without adequate notice and failing to prevent unauthorized disclosure. Plaintiff asserts related claims under the UCL and CLRA based on the same conduct and violation of, *inter alia*, the CCPA. Plaintiff also alleges negligence, invasion of privacy, and unjust enrichment.

While these initial CCPA-related cases remain at the earliest stages, they demonstrate the ways in which consumer plaintiffs will use the CCPA in class actions. Notably, however, not all consumer privacy complaints filed since January incorporated the CCPA. Indeed, two consumer complaints filed in March 2020 in the Northern District of California make allegations arising from a consumer data breach, but do not include any claim under (or even reference to) the CCPA.

***I.C., a minor by and through his natural parent, Nasim Chaudhri and Amy Gitre v. Zynga, Inc., Case No. 3:20-cv-01539 (N.D. Cal.); Carol Johnson and Lisa Thomas v. Zynga, Inc., Case No. 3:20-cv-02024 (N.D. Cal.)***

On March 3, 2020, Plaintiffs Amy Gitre and I.C. filed a putative class action Complaint arising from video game manufacturer Zynga’s alleged failure to protect PII of its users, including both adults (Gitre) and minors (I.C.). Plaintiffs filed a fourteen-count Complaint that includes statutory and common law claims arising from the alleged failure to properly secure account holders’ PII. In September 2019, a hacker publicly claimed to have breached Zynga’s database and was able to extract information concerning 218 million users. The breach is alleged to have included users from some of Zynga’s most popular games: Words With Friends; Draw Something; and OMGPOP. On September 12, 2019, Zynga posted a “Player Security Announcement” that confirmed the breach.

Plaintiffs seek to represent a nationwide class of: “All individuals in the United States whose PII was obtained or maintained by Zynga and compromised as a result of the Zynga data breach described herein” as well as adult and minor sub-classes. The causes of action include: negligence; negligent misrepresentation; negligence per se (under Section 5 of the FTC Act); unjust enrichment; violation of state data breach laws (including failure to safeguard data and failure to provide adequate notice of the breach); intrusion upon seclusion; and declaratory judgment (seeking an injunction compelling proper security of PII). There are no references to, or causes of action under, the CCPA.

On March 23, a follow-on suit was filed in the same court raising similar allegations. The Plaintiffs, Carol Johnson and Lisa Thomas, seek an identical nationwide class as well as Missouri and Wisconsin sub-classes, based on the citizenship of the Plaintiffs. The Complaint asserts a narrower list of causes of action regarding negligence, negligence per se, unjust enrichment, and declaratory judgment. Again, there are no references to, or causes of action under, the CCPA.

We will continue to monitor the various claims, as well as court decisions in CCPA litigations. If you

have any questions about defending and/or preparing for a potential privacy consumer class action, please reach out to our team.

