AN A.S. PRATT PUBLICATION
OCTOBER 2020
VOL. 6 • NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 **NUMBER 8** **OCTOBER 2020**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [245] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2020–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Number of Lawsuits Filed Under the California Consumer Privacy Act Continues to Grow

By Alysa Zeltzer Hutnik, Paul A. Rosenthal, Taraneh Marciano, and William Pierotti *

The authors provide an update on cases filed earlier this year under the California Consumer Privacy Act.

January 1, 2020 was the effective date for the California Consumer Privacy Act ("CCPA"), and private litigants wasted no time in filing consumer-related causes of action under the new law.

This article provides an update on material developments in that first wave of claims and reports on additional private lawsuits commenced in the first half of the year. It further categorizes the recently-filed cases based on those stemming from a data breach versus not. In the latter category, the cases are further split based on the underlying alleged violations – second quarter, non-breach based claims related to the disclosures and opt-out mechanisms required by the CCPA, as well as the scope of "personal information" covered by the CCPA.

UPDATE ON CERTAIN CASES FILED IN THE FIRST QUARTER OF 2020

Consolidated Zoom Cases, **Case No. 5:20-cv-02155 (N.D. Cal.)**

Since the beginning of the second quarter of 2020, at least 13 putative consumer class actions have been filed against Zoom in federal court. Of those, 12 allege direct violations of the CCPA and one alleges violation of California's Unfair Competition Law ("UCL") based on noncompliance with the CCPA. At least two additional putative consumer class actions have been filed against Zoom in state court on behalf of California consumers. Of those, one alleges direct violations of the CCPA and the other alleges violations of the UCL based on noncompliance with the CCPA.

* Alysa Zeltzer Hutnik, a partner in the Washington, D.C., office of Kelley Drye & Warren LLP, chairs the firm's Privacy and Information Security practice. Paul A. Rosenthal, a partner in the firm's office in Parsippany, New Jersey, focuses his practice on defending public and private companies in complex commercial litigation matters. Taraneh Marciano, resident in the firm's New York office, is special counsel in the firm's Intellectual Property and Privacy Litigation practice groups. William Pierotti is an associate in the firm's New York office. The authors may be contacted at ahutnik@kelleydrye.com, paulrosenthal@kelleydrye.com, tmarciano@kelleydrye.com, and wpierotti@kelleydrye.com, respectively.

All of the federal consumer cases against Zoom have been consolidated in the Northern District of California as related cases under the caption *In Re: Zoom Video Communications Inc. Privacy Litigation*, Case No. 5:20-cv-02155-LHK. On June 30, 2020, Judge Lucy H. Koh issued an order appointing nine attorneys to the Plaintiffs Steering Committee, triggering a July 30, 2020 deadline for the plaintiffs to file a consolidated complaint.

***Consolidated Hanna Andersson Cases,* Case No. 3:20-cv-01572 (N.D. Cal.)**

Since the February 3 filing of the original complaint against Hanna Anderson and Salesforce, at least one additional complaint was filed against the defendants. The two cases were consolidated by Judge Edward M. Chen on May 5, 2020 under the caption *In Re: Hanna Andersson And Salesforce.com Data Breach Litigation*, Case No. 3:20-cv-01572-EMC. An amended consolidated complaint seeks to create three classes composed of:

- Nationwide consumers;
- California consumers; and
- Virginia consumers.

The original complaint, filed by California consumer Bernadette Barnes, did not include a cause of action under the CCPA and only referenced it as a trigger for a UCL claim. The consolidated complaint directly alleges a cause of action for violations of the CCPA on behalf of the California Class. Plaintiffs allege that they complied with the notice and cure provision of the CCPA, which provides that "[a]ctions pursuant to [the CCPA] may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated."[1]

Under the statute, covered entities that receive such notice can avoid liability to individual and class consumers by "actually cur[ing] the noticed violation and provid[ing] the consumer an express written statement that the violations have been cured and that no further violations shall occur."[2] The *Hanna Andersson* plaintiffs allege that defendants failed to cure the underlying data breach or provide an express written statement that the violations were cured within 30 days of the plaintiffs' written notice, and the plaintiffs therefore seek statutory damages of $100 to $750 per violation of the CCPA.

As many of the cases below highlight, there is a trend in CCPA litigation where plaintiffs file their claims prior to expiration of the 30-day cure period with the (sometimes stated) intention that they will amend their complaints to demand statutory damages once the requisite time period runs.

[1] Cal. Civ. Code § 1798.150(b).
[2] *Id.*

CASES FILED IN THE SECOND QUARTER BASED ON DATA BREACHES

***Rahman v. Marriott International,* Case No. 8:20-cv-00654 (C.D. Cal.)**

On April 3, 2020, California consumer Arifur Rahman filed a putative class action against hospitality company Marriott International. Marriott allegedly collected personally identifiable information ("PII") from guests and loyalty members, including contact details such as name, mailing address, email address, and phone number; personal details such as employer, gender, and birthday; and preferences such as type of stay/room and language. This information was subsequently accessed without authorization through the login credentials of two employees, resulting in a breach affecting 5.2 million customers. Marriott announced the breach on March 31, 2020.

Plaintiff seeks to represent "[a]ll persons in the State of California whose Personal Information was stolen, disclosed, or accessed without authorization in the data breach incident." Plaintiff alleges that Marriott violated the CCPA by failing to establish adequate security measures, which resulted in the disclosure of unencrypted and unredacted PII.

On June 29, 2020, plaintiff filed an amended complaint naming additional plaintiffs; stating that "[m]ore than 30 days have elapsed, but Marriott has not actually cured the noticed violations, nor has it provided the Class with an express written statement that the violations have been cured and that no further violations shall occur"; and demanding statutory damages under the CCPA.

***Consolidated Ambry Genetics Cases,* Case No. 8:20-cv-00791 (C.D. Cal.)**

At least four putative consumer class action cases have been filed against Ambry Genetics ("Ambry"), a company that provides genetic testing services, following an alleged data breach in January 2020. The breach allegedly resulted in unauthorized access to customer PII and Protected Health Information ("PHI"). Ambry allegedly failed to report the breach to the government until March 2020 and did not report the breach to customers under April 2020.

On June 16, 2020, Chief Judge Cormac J. Carney consolidated these cases under the caption *Cercas v. Ambry Genetics Corp.*, Case No. 8:20-cv-00791. The parties were required to submit a proposed case management order by August 10, 2020 setting out deadlines for, among other things, the filing of a consolidated complaint.

While the complaint in the lead case *Cercas* does not allege a CCPA cause of action, the remaining three complaints – *Brodsky v. Ambry Genetics*, Case No. 8:20-cv-00811 (C.D. Cal.); *Pascoe v. Ambry Genetics*, Case No. 8:20-cv-00838 (C.D. Cal.); and *McMurphy v. Ambry*, Case No. 8:20-cv-00904 (C.D. Cal.) – do allege violations of the CCPA, either directly or as a predicate to claims under the UCL.

***Gupta v. Aeries,* Case No. 8:20-cv-00995 (C.D. Cal.)**

On May 28, 2020, California resident Anurag Gupta and his two minor children filed a putative class action against Aeries, which provides student data management services to schools. Aries holds sensitive student information including academic, grade and disciplinary records, as well as students' medical information. They also hold parent- and guardian-related data and records associated with their students' accounts. Plaintiffs allege that Aeries' insufficient data security policies permitted unauthorized access to at least 166 servers, resulting in unauthorized access to thousands of student and parent records.

The plaintiffs seek to represent four classes of claimants – nationwide and California classes of parents and students. Specifically, plaintiff Gupta seeks to represent a nationwide class composed of "[a]ll students, parents, and guardians in the United States whose PII was compromised in the Data Breach" and a California subclass composed of "[a]ll students, parents, and guardians in California whose PII was compromised in the Data Breach." Plaintiff Gupta's minor children, D.G. and V.G., seek to represent a nationwide minor subclass composed of "[a]ll minor students in the United States whose PII was compromised in the Data Breach, as well as all adult individuals in the United States who provided PII to Aeries while they were minor students and had their PII compromised in the Data Breach" and a California minor subclass composed of "a[] ll minor students in California whose PII was compromised in the Data Breach, as well as all adult individuals in California who provided PII to Aeries while they were minor students and had their PII compromised in the Data Breach."

Plaintiffs allege violation of the CCPA as a standalone claim on behalf of the California subclasses. Plaintiffs allege that they served the letter notice required under the CCPA, and state that they plan to amend their claims to demand statutory damages once they receive a response. No amended complaint has yet been filed. Plaintiffs also allege violation of the CCPA as one of the predicates to a UCL claim brought on behalf of all the classes and subclasses.

***Atkinson v. Minted,* Case No. 3:20-cv-03869 (N.D. Cal.)**

On June 11, 2020, California consumers Melissa Atkinson and Katie Renvall filed a putative class action against online marketplace Minted. Plaintiffs allege that Minted's insufficient data security measures permitted hackers to exfiltrate five million customer records, including allegedly unredacted and unencrypted consumer names combined with user names and passwords.

Plaintiffs seek to represent two classes – a nationwide class composed of "[a]ll individuals whose [PII] was compromised in the Data Breach" and a California class composed of "[a]ll persons residing in California whose [PII] was compromised in the Data Breach."

On behalf of the California class, Plaintiffs allege two claims for: (1) violation of the CCPA through "failing to prevent Plaintiffs' and Class members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information," and (2) violation of the UCL based upon the CCPA violation.

Plaintiffs allege that they sent the required notice to cure; however, because the breach already occurred and the data was already disseminated, it is impossible to cure the violation of the CCPA. Despite that argument, the plaintiffs stated that after expiration of the cure period they would amend their complaint to assert actual damages and statutory damages of $750 per customer record, but have yet to do so.

CASES FILED IN THE SECOND QUARTER NOT BASED ON DATA BREACHES

Insufficient Disclosures

Sweeney v. Life on Air, Inc. & Epic Games, Inc., Case No. 3:20-cv-00742 (S.D. Cal.)

On April 17, 2020, California consumer Heather Sweeney filed a putative class action against Life on Air, Inc. and its parent company Epic Games, developer of the social networking application Houseparty. Plaintiff alleges that defendants disseminate PII to third parties, including Facebook, without consent or disclosure, so that advertisements can be targeted to the users.

Plaintiff seeks to represent a class of "[a]ll citizens of the State of California who accessed the Houseparty application . . . from January 1, 2020 to April 17, 2020." Plaintiff alleges that defendants violated the CCPA by failing to:

- Notify users that they were collecting and disseminating PII;
- Provide notice of the right to opt out;
- Provide a clear and conspicuous link to a page titled "Do Not Sell My Personal Information" where they would be able to opt out; and
- To "use any personal information collected from the consumer in connection with keeping their personal information private" in violation of Cal. Civ. Code § 1798.135(a)(B)(6).

On July 10, 2020, the defendants filed a motion to compel arbitration or, in the alternative, to transfer the case to the Northern District of California. Defendants argue that the terms of service, which plaintiff agreed to in using the application, contain both an enforceable arbitration clause and a forum-selection clause designating the Northern District of California as the proper venue for any litigation.

G.R. v. TikTok, Case No. 2:20-cv-04537 (C.D. Cal.)

On May 20, 2020, California minor G.R. filed a putative class action against video social networking application provider TikTok and parent company ByteDance, Inc. Plaintiff alleges that TikTok scans every video uploaded to the application for faces, extracts biometric identifiers of each face, and uses the data to create and store a template of each face without disclosing this process to its users. TikTok then allegedly disseminates the biometric identifiers to third parties without the requisite notice.

Plaintiff seeks to represent a class composed of "[a]ll minor persons who registered for or used the TikTok app from at least May 14, 2017 to the present." Plaintiff alleges that California law applies to all class members based on TikTok's California-based U.S. headquarters. Plaintiff asserts claims for violations of the CCPA based on the defendants' failure to provide required notice to users about the application's collection and use of their data and of their right to opt out. Plaintiff does not allege that the requisite notice and opportunity to cure under the CCPA were provided. Plaintiff also alleges violation of the CCPA as a predicate for its UCL claim.

Failure to Provide Opt-Out

Sweeney v. Life on Air, Inc. & Epic Games, Inc., Case No. 3:20-cv-00742 (S.D. Cal.)

In *Sweeney*, discussed above, the plaintiff alleges that, in addition to failing to provide users with sufficient notice regarding the collection and use of their personal information, including their right to opt out, the defendants also violated the CCPA by failing to provide a clear and conspicuous link to a page titled "Do Not Sell My Personal Information" where users would be able to opt out.

Scope of "Personal Information"

Shay v. Apple, Case No. 37-2020-00017475 (San Diego Super. Ct.)

On May 28, 2020, California consumer Rachel Shay filed a putative class action against Apple. Plaintiff alleges that Apple markets defective gift cards that are easily electronically compromised by thieves. According to the plaintiff, the gift cards have "Personal Identification Number[s]" ("PINs") that are "covered with silver scratch off tape," and that, upon information and belief, these PINs are "'personal information' associated with and/or reasonably linked . . . with the purchasing consumer upon activation." Plaintiff alleges a direct violation of the CCPA and seeks to represent a class composed of "[a]ll consumers in the United States who purchased an Apple gift card wherein the funds on the Apple gift card was [*sic*] redeemed prior to use by the consumer" and a California subclass based on the same definition.