CCPA Privacy and Cybersecurity Advisory:

A CCPA Private Right of Action on the Horizon: Class action complaints test whether plaintiffs can sue for any violation of the CCPA

April 10, 2020

A CCPA Private Right of Action on the Horizon: Class action complaints test whether plaintiffs can sue for any violation of the CCPA

by David Keating, Jim Harvey and Daniel Felz

*　　*　　*　　*　　*　　*

While much of the privacy community has been focused – for good reason – on the COVID-19 public health emergency, plaintiffs' counsel have started to lay the groundwork for a broad private right of action under the California Consumer Privacy Act[1] (the "CCPA").

The first part of this article provides an overview of how the CCPA addresses private rights of action. The second section summarizes recent class action complaints that attempt to use CCPA violations as the basis for class-wide claims, either via claims asserted directly under the CCPA or through the California Unfair Competition Law. The third and final part provides suggestions for prioritizing activity in CCPA compliance programs in this new litigation environment.

Part One: The CCPA and Private Rights of Action

The California Consumer Privacy Act was the end product of a negotiation with the backers of a proposed ballot initiative[2] that, if successful, would have granted California residents the right to be notified of and to opt out from sales of personal information.[3] One of the primary objectives of the business community in supporting the negotiations was to eliminate a proposed private right of action.[4] The final statute, a product of compromise on both sides, promised to limit any private right of action to claims for certain data security incidents resulting from a failure to comply with pre-existing standards of California law.[5] Privacy attorneys and litigators were, however, quickly skeptical about whether the compromise language would be effective to preclude broader class action suits.

1. A Private Right of Action under the CCPA with Statutory Damages for Data Breach.

Section 1798.150(a) of the CCPA expressly establishes a private right of action for consumers "whose nonencrypted and 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 to

[1] Cal. Civ. Code §§ 1798.100 to 1798.198.

[2] Californians for Consumer Privacy, www.caprivacy.org.

[3] *See* The California Consumer Privacy Act of 2018, Ballot Initiative No. 17-0027, draft stamped as received by California Attorney General on Oct. 9, 2017 available at https://oag.ca.gov/system/files/initiatives/pdfs/17-0027%20%28Consumer%20Privacy%29_1.pdf.

[4] *See* California Senate, *Senate Judiciary Committee, Tuesday, April 9th, 2019* at 3:34:00-3:39:25, available at https://www.senate.ca.gov/media/senate-judiciary-committee-20190409/video

[5] Cal. Civ. Code § 1798.81.5.

protect the personal information . . . ."[6] While California residents already had a right to bring private suits arising from certain types of security incidents,[7] the CCPA for the first time established statutory damages for these claims.[8]

2. Is There a Private Right of Action for Violations of the CCPA's Privacy Standards?

The CCPA appears, at first glance, to prohibit private rights of action outside the 1798.150(a) information security breach scenario. The statute provides that "[n]othing in this title shall be interpreted to serve as the basis for a private right of action under any other law."[9] From the time the law was first enacted, however, commentators have noted that this language may not be sufficient to preclude class actions brought under the California Unfair Competition Law[10] (the "UCL") based on general violations of the privacy standards of the CCPA.[11]

The UCL empowers private litigants to initiate class action proceedings to enjoin unlawful, unfair, and fraudulent business practices and to seek restitution and recovery of attorney's fees.[12] Violations of a statute "may serve as the predicate for a UCL cause of action" for alleged unlawful conduct.[13] A UCL claim based on unlawful conduct evidenced by the violation of a statute will not be precluded unless the statute *in question "actually 'bar[s]' the action or clearly permit[s] the conduct."*[14]

The issue then is whether the CCPA "actually 'bar[s]' " a UCL claim based on a violation of the CCPA. The failure to squarely address this question in the new law was raised by interest groups during lobbying processes in 2018 and 2019.[15] The State Assembly and Senate have thus far declined to clarify the issue. At the same time, a bill backed by Attorney General Xavier Becerra which would have established a direct private right of action, designated Senate Bill 561, failed to attract sufficient support to come to a floor vote last year and died in committee.[16] Comments in the Senate during the debate on SB 561 suggested the legislature had intended specifically not to authorize private litigation beyond security-related claims under Section 1798.150(a).[17]

[6] Cal. Civ. Code § 1798.150(a).
[7] Cal. Civ. Code § 1798.84(a).
[8] Cal. Civ. Code § 1798.150(a).
[9] Cal. Civ. Code § 1798.150(c).
[10] Cal. Bus. & Prof. Code §§ 17200 to 172010.
[11] *See* Bo Phillips and Gillian Clow, *Privacy & Data Security Advisory: An Update on the California Consumer Privacy Act and its Private Right of Action* (Sept. 12, 2018), available at https://www.alston.com/en/insights/publications/2018/09/california-consumer-privacy-act.
[12] Cal. Bus. & Prof. Code § 17203.
[13] *Rose v. Bank of America, N.A.*, 304 P.3d 181, 183 (Cal. 2013).
[14] *Id.* at 186.
[15] *See* Letter of Various Business and Industry Associations to Cal. State Sen. Bill Dodd (Aug. 6, 2018), available at https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2790&context=historical.
[16] https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=201920200SB561
[17] California Senate, *Senate Judiciary Committee, Tuesday, April 9th, 2019* at 3:34:00-3:39:25, available at https://www.senate.ca.gov/media/senate-judiciary-committee-20190409/video.

Part Two: Recent CCPA Litigation via the California Unfair Competition Law

A series of recent class action complaints are testing the theory that the UCL affords private plaintiffs the ability to bring class actions for violations of the CCPA beyond the limited right to bring claims for data breach matters under Section 1798.150(a). Whether plaintiffs have a right to initiate private litigation under the CCPA therefore appears bound to be decided in the courts.

1. *Burke v. Clearview AI, Inc.*[18]

The plaintiffs filed a class action complaint on February 27, 2020, following press reports of allegations that the defendant Clearview AI had collected billions of images from sources across the Internet and processed the images in a manner designed to create biometric faceprints. The plaintiffs pled claims under the Illinois Biometric Privacy Information Act[19] and for common law commercial appropriation and unjust enrichment. But Count I of the complaint seeks relief under the UCL for the defendant's alleged violation of the CCPA's "notice at collection" requirements set forth in Section 1798.100(b).

2. The *Zoom* Lawsuits.

Plaintiffs have filed class action complaints against Zoom in three separate proceedings[20] since late March that arise from well-publicized reports concerning Zoom's alleged data practices. All three actions are based on allegations that the Apple iOS version of Zoom's videoconferencing app allegedly contained a software development kit that sent user information to Facebook, and on alleged flaws in Zoom's information security program and controls. The claims allege that (a) the Zoom mobile app sent data to Facebook each time a user used the app, even if the user did not have a Facebook account, and (b) Zoom did not notify app users of the collection of this data or the sharing of the data with Facebook. *Taylor* and *Johnston* further allege that Zoom failed to notify users of an alleged right to opt out from this information sharing with Facebook pursuant to the CCPA's "do not sell" standards.[21]

- In *Cullen v. Zoom*, the plaintiffs have asserted claims against Zoom under California's Unfair Competition Law (UCL).[22] The claims allege that "Zoom collected [users'] 'personal information' as defined in the CCPA and failed to inform [them] of the same at or before the point of collection," thus "violat[ing] the CCPA."[23] Plaintiffs allege this made Zoom's iOS app an "unlawful and unfair business practice[]" actionable under the UCL.[24]

[18] No. 20-cv-0370, Dkt. No. 1 (S.D. Cal. filed Feb. 27, 2020).

[19] *See* 740 Ill. Compiled Statutes 14/1 *et seq.*

[20] *See Johnston v. Zoom Video Comms., Inc.*, No. 5:20-cv-2376, Dkt. No. 1 (N.D. Cal. filed Apr. 8, 2020); *Taylor v. Zoom Video Comms., Inc.*, No. 5:20-cv-2170, Dkt. No. 1 (N.D. Cal. filed Mar. 31, 2020); *Cullen v. Zoom Video Comms., Inc.*, No. 5:20-cv-2155, Dkt. No. 1 (N.D. Cal. filed Mar. 30, 2020);

[21] *See Johnston*, *supra*, at para. 103 (asserting CCPA claim on grounds that Zoom allegedly "fail[ed] to provide notice to [users] of their right to opt out of the disclosure or use of their personal information to third parties"); *Taylor*, *supra*, at para. 132 (asserting CCPA claim on grounds that Zoom allegedly "fail[ed] to provide notice to its customers of their right to opt-out of the disclosure of their PII to unauthorized parties like Facebook").

[22] *See Cullen*, *supra*, at paras. 41-52.

[23] *Cullen*, *supra*, at para. 48.

[24] *Cullen*, *supra*, at para. 43.

- In contrast, the plaintiff in *Taylor v. Zoom* asserts a direct CCPA claim without referencing or explaining the inapplicability of the restriction on private rights of action in Section 1798.150(c).[25] The complaint alleges Zoom (a) "did not notify [users] that it was disclosing their PII to unauthorized parties like Facebook," thus not providing the notice at or before the point of collection required by Cal. Civ. Code § 1798.100(b), and (b) failed to provide users with the notice required under Cal. Civ. Code § 1798.120(b) of their "right to opt out of the disclosure or use of their personal information to third parties" which amounts to a 'sale' as defined in the CCPA.[26]

- The complaint in *Johnston v. Zoom* asserts similar claims to those in *Taylor*. The *Johnston* plaintiffs also assert a direct CCPA claim against Zoom without addressing the inapplicability of the restriction on private rights of action in Section 1798.150(c).[27] The complaint alleges that Zoom (a) failed to provide the "required notice" under Cal. Civ. Code § 1798.100(b) because it "did not notify [users] that it was disclosing their PII to unauthorized parties like Facebook," and (b) failed to provide users with the notice required under Cal. Civ. Code § 1798.120(b) of "their right to opt-out of the disclosure of their PII to unauthorized parties like Facebook", as well as any "opportunity to opt out before it provided their PII" to such third parties.[28]

We note two common themes in *Cullen*, *Taylor*, and *Johnston*:

A. **The CCPA "notice at collection" has evolved from a debate topic to a live litigation risk.** For many companies, the concept of "notices at collection" separate from an online privacy policy appeared relatively late in CCPA compliance efforts. The CCPA contains parallel provisions on consumer disclosures about privacy practices. Section 1798.130(a)(5) requires businesses to post an "online privacy policy" on their website, while Section 1798.100(b) requires businesses to make more limited disclosures to consumers "at or before the point of collection." Initially after the CCPA's passage, this raised questions about whether the CCPA contained two separate notice requirements: an initial "notice at collection," supplemented by a more fulsome privacy policy available online. A number of observers maintained that an online privacy policy fully satisfied CCPA notice obligations.

    - The Draft CCPA Regulations issued by the California Attorney General's Office ("AG's Office") in October 2019[29] established separate rules for "notices at collection," making clear that the Attorney General interprets the CCPA to require these notices to be separate and distinct from traditional privacy policies.

[25] *See Taylor*, *supra*, at p. 22 paras. 129-133.
[26] *Taylor*, *supra*, at p. 22 para. 131-132.
[27] *See Johnston, supra*, at paras. 100-104.
[28] *See Taylor, supra*, at p. 22-23, paras. 131-132.
[29] The original October 2019 draft of the proposed CCPA Regulations can be found at the California Attorney General's dedicated CCPA website, https://oag.ca.gov/privacy/ccpa. All citations to the Draft Regulations in this Advisory use the text from the most recent version as of the date of this Advisory, i.e. the version released March 11, 2020 by the Attorney General and available at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-second-set-clean-031120.pdf (hereinafter the "Draft Regulations").

- The Zoom lawsuits suggest that the "notice at collection" standard has moved from an interpretive debate to a 'live' litigation risk. Each suit focuses specifically on Zoom's alleged failure to provide a notice to app users at the point of collection – effectively a just in time notice – of the data collected and shared with Facebook.

B. **Does the failure to provide 100(b) notice at collection result in "unauthorized access" to personal information for data breach litigation purposes?**

As discussed, the CCPA grants consumers a private right of action when certain personal information has been "subject to an unauthorized access . . . or disclosure" as a result of a business's failure "to implement and maintain reasonable security procedures."[30] The common understanding of this language has been that it intended to tie the ability to bring CCPA civil claims to data breaches. The *Zoom* lawsuits indicate, however, that the plaintiffs' bar may be attempting to cast the failure to provide a "notice at collection" as giving rise to actionable security violations. All three suits are suggesting Zoom's alleged failure to notify users that data could be shared with Facebook, identify the sharing as a "sale" of personal information, and provide an opportunity for users to opt out amounted to sharing data with an "unauthorized party."[31]

- ➢ In other words, non-notified sharing that amounts to a sale under the CCPA is being characterized as "unauthorized" sharing equivalent to a security failure.

Part Three: Takeaways for Privacy Counsel and Professionals.

1. <u>Notices at Collection are a Flash Point of Risk.</u>

Violation of the CCPA's new "notice at collection" requirement are an attractive basis for class action complaints due to the ability of plaintiff's counsel to multiply the violation by the number of times consumers have visited the Web site, downloaded the mobile app, or used relevant features within the app. We suspect this is why alleged violations of this requirement feature so prominently in the Clearview AI and Zoom suits. But truly effective compliance with the notice at collection requirement can be highly complicated and resource intensive for businesses.

Identifying all potential consumer touchpoints where data might be collected can require significant technical due diligence and investigation of direct person-to-person interactions in brick-and-mortar settings. Privacy teams often have limited bandwidth for detailed technical investigations and IT functions can quickly lose patience with probing privacy counsel and staff.

We have worked with many clients to create a catalogue or index of data collection channels with references to point-of-collection notices, with an emphasis on simplicity. We recommend tightly integrating this work with ongoing privacy assessment processes to ensure notices remain complete and accurate over time.

[30] Cal. Civ. Code § 1798.150(a)

[31] *See, e.g., Taylor, supra*, at para. 132

2. <u>We have to understand, at a technical level, how SDKs interoperate with consumer-facing mobile apps</u>.

   Software development kits or "SDKs" integrated into mobile apps are a rough equivalent from a data collection and targeting perspective to cookies, pixels, and other tracking technologies on traditional Web sites. We have long cautioned of the need to understand in detail how third party SDKs interoperate with mobile apps to ensure the continued accuracy of disclosures in privacy notices. The alleged failure to do so is at the core of the recent Zoom class action complaints.

   Consider using the app maintenance and update cycle to require regular scans and reviews of app components prior to enterprise release. Regular reviews can also serve as a springboard for ongoing documentation of app functionalities and SDKs, as well as the measures taken to ensure their compliance.

3. <u>We have to understand, at a technical level, whether and how all consumer products, equipment components and other tangible items distributed by the business collect and share data</u>.

   The sale and distribution of networked products has exploded. Businesses may now find themselves distributing consumer products, equipment components, or even giveaway items that have embedded sensors collecting data from end users or regarding the location and environments in which the products are deployed. Much of the discussion around such Internet of Things or "IoT" products involves the security they provide for data they collect from users. The allegations in the *Zoom* lawsuits suggest that notice-at-collection should be an equal part of this discussion.

   - IoT products invariably collect data as part of their standard functioning, which can often be linked to a purchaser or user; as such, IoT devices may be collecting personal information within the meaning of the CCPA. This may give rise to "notice at collection" obligations that, if not complied with, would potentially serve as a basis for complaints like *Taylor* and *Cullen*.

   - Moreover, IoT products increasingly share data with a number of third parties, including those who may use data for digital analytics or advertising. The theory in *Taylor* and *Cullen* is that if such sharing is not adequately disclosed to consumers, it can be characterized as a security violation, i.e. sharing of data with unauthorized parties. A similar theory also appeared in a recent CCPA lawsuit brought against video-doorbell manufacturer Ring, with plaintiffs alleging that Ring "concealed its commercial tracking and sharing of customers' PII with third parties," which contributed to Ring doorbells having "inadequate privacy and security measures."[32] *Taylor* and *Johnston* also contend an independent violation based on the failure to notify consumers of the right to opt out of the sharing as an alleged CCPA "sale" of personal information.[33]

[32] *Sheth v. Ring*, No. 2:20-cv-1538, Dkt. No. 2 at para. 90 (C.D. Cal. filed Feb. 18, 2020).

[33] *See Johnston*, *supra*, at para. 103; *Taylor, supra*, at p. 22 para. 132.

We recommend as initial steps focusing on high profile products and marketing initiatives that result on large-scale distribution of products, compiling details regarding networked devices, zeroing in on including notices in customer terms and conditions, and integrating the work going forward with a privacy assessment process for new products / R&D and the digital marketing team.

*   *   *   *   *   *

For more information, contact the authors of this article, David Keating, Jim Harvey, or Daniel Felz, or your attorney on the Alston & Bird Privacy & Security Team.