AN EPUBLICATION OF THE LOS ANGELES COUNTY BAR ASSOCIATION

LACBA

PRIVACY AND CYBERSECURITY SECTION

Section Home Page
click here ›

JUNE 2020

Back to June 2020 issue

Recent Lawsuits Against Zoom Test the Scope of the CCPA's Private Right of Action

JUSTIN T. YEDOR and BETHANY G. LUKITSCH, McGuireWoods LLP

On March 30, 2020, the first of several putative class action lawsuits was filed against videoconferencing service Zoom relating to its data privacy practices.[1] While the exact allegations vary from case to case, the first-filed action, *Cullen v. Zoom Video Communications, Inc.*, No. 5:20-cv-02155 (N.D. Cal. Mar. 30, 2020), focuses on Zoom's alleged transfer of users' personal information to Facebook without prior notice. Plaintiffs brought six causes of action against Zoom, including an independent claim for violation of the California Consumer Privacy Act of 2018 (the "CCPA").[2] Consequently, the Zoom cases may be the first to test whether the CCPA's private right of action is limited to data breaches or whether a more expansive reading is permissible.

Section 1798.150 of the California Civil Code allows consumers to recover statutory or actual damages as well as injunctive relief when:

> nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, 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.

While many commenters (and the CCPA's authors[3]) have said that § 1798.150 is limited to data breaches, it appears the *Cullen* plaintiffs interpret it more broadly as they do not claim Zoom suffered a data breach in the traditional sense of that term. Instead, they allege that their "personal information was subjected to unauthorized disclosure . . . through the Zoom App where personal information was regularly collected and

---

[1] *See Cullen v. Zoom Video Comm'ns, Inc.*, No. 5:20-cv-02155 (N.D. Cal. Mar. 30, 2020); *Taylor v. Zoom Video Comm'ns, Inc.*, No. 5:20-cv-02170 (N.D. Cal. Mar. 31, 2020); *Johnston v. Zoom Video Comm'ns, Inc.*, No. 5:20-cv-02376 (N.D. Cal. Apr. 8, 2020); *Hurvitz v. Zoom Video Comm'ns et al.*, No. 2:20-cv-03400 (C.D. Cal. Apr. 13, 2020); *Ohlweiler v. Zoom Video Comm'ns, Inc.*, No. 2:20-cv-03165 (C.D. Cal. Apr. 3, 2020); *Kondrat et al. v. Zoom Video Comm'ns, Inc.,* No. 5:20-cv-02520 (N.D. Cal. Apr. 13, 2020).

[2] Plaintiffs also allege violation of the CCPA as a predicate statutory violation for their claim under the California Unfair Competition Law, CAL. BUS. & PROF. CODE § 17200, *et seq*.

[3] *See, e.g., Author's Statement Re: SB 1121, Assembly Committee on Privacy and Consumer Protection* (Aug. 28, 2018) (stating that, under the proposed revision to the CCPA, the private right of action "applies only to the data breach portion of the CCPA").

sent to Facebook and possibly other third parties without authorization."[4] Specifically, the *Cullen* plaintiffs allege that when users install or open the Zoom app, "the users' mobile OS (operating system) type and version, the device time zone, the device model and the device's unique advertising identifier" are transferred to Facebook without their knowledge.[5]

The *Cullen* Complaint describes Zoom's actions as an "unauthorized disclosure," and alleges that if Zoom had followed "practices appropriate to the nature of the information," it would not have been transferred to Facebook without prior notice to the plaintiffs.[6] The CCPA does not define "unauthorized disclosure,"[7] so it will fall to the Court to decide exactly what that term means.

Zoom will likely argue that the transfer of information to Facebook is not "an unauthorized disclosure" under § 1798.150 because it did not result from "the business's violation of the duty to implement and maintain reasonable security measures and practices." Plaintiffs will likely point out that § 1798.150 does not actually include the terms "data breach" or "security breach" when describing the facts that can support a cause of action, so it is arguable that a claim exists in a wider array of circumstances. On the other hand, Section 1798.150 cites directly to California's data breach notification law for businesses, CIV. CODE § 1798.81.5. It is also noteworthy that Section 1798.150 uses a different definition of "personal information" from that used elsewhere in the CCPA, and that the information identified in the *Cullen* Complaint does not appear to be encompassed within this definition.[8]

Regardless of which side's arguments ultimately carry the day, *Cullen* and the other Zoom cases will be of interest to both plaintiffs' lawyers and defense counsel litigating data privacy issues in California. More broadly, any ruling from the Court interpreting the scope of the CCPA's private right of action would provide much needed guidance for practitioners, businesses, and consumers trying to understand the new rights and liabilities provided by the CCPA.

---

[4] *Cullen*, No. 5:20-cv-02155, Compl. ¶ 35.

[5] *Id.* ¶ 16.

[6] *Id.* ¶ 34.

[7] Nor does the CCPA define the terms "access," "exfiltration," or "theft."

[8] The *Cullen* Plaintiffs allege that Zoom transferred "the users' mobile OS (operating system) type and version, the device time zone, the device model and the device's unique advertising identifier" to Facebook. *Cullen*, No. 5:20-cv-02155, Compl. ¶¶ 16, 20. By contrast, CIV. CODE § 1798.81.5(d)(1)(A) defines "personal information" as:

> An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
> (i) Social security number.
> (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
> (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
> (iv) Medical information.
> (v) Health insurance information.
> (vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.