



LEGAL UPDATES

What Businesses Can Learn From the Privacy Lawsuit Filed Against Zoom

Just as the COVID-19 virus sent us scurrying to video conferences as an antidote to social and professional isolation, a class action lawsuit was filed against Zoom alleging that the app improperly collects users' personal information and discloses it to third parties.

04/28/2020 | 4 minute read

Erika Gasaway and **Celine Guillou**

Just as the COVID-19 virus sent us scurrying to video conferences as an antidote to social and professional isolation, a class action lawsuit was filed against Zoom alleging that the app improperly collects users' personal information and discloses it to third parties. According to the allegations in the lawsuit, the Zoom app notifies Facebook when any Zoom user opens the app and provides details about the user's device, the time zone and city from which the user connects, the user's service provider, and the user's unique advertising identifier (built into users' devices). The information is allegedly transmitted to Facebook regardless of whether the user has a Facebook account.

Did Zoom users in California have notice and opportunity to opt-out of Zoom collecting and selling their personal information? Assuming for the moment that the allegations in the lawsuit are true, the answers to those questions will help determine whether Zoom faces any liability for violating the new and as-yet-untested California Consumer Privacy Act ("CCPA"). However, that question might not be answered if the plaintiffs fail to convince the Court that a class action is proper under the circumstances. Namely, before the expiration of the 30-day notice and opportunity for Zoom to cure its violations has passed. Zoom would be well-advised to bring a relatively early motion to test the validity of the plaintiffs' claim for attorney fees. The statute is not clear on that point, and the inability to recover attorney's fees could very well make it impossible for the plaintiffs to pursue the suit.

The main allegation of the class action complaint is that Zoom violated Section 1798.150(a) of the CCPA by failing to prevent the plaintiff's and the class members' non-encrypted and non-redacted personal information from unauthorized disclosure as a result of Zoom's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect their personal information. In other words, by passing the information along to Facebook unbeknownst to users or without providing a choice, the plaintiffs allege that Zoom enabled an unauthorized access of unencrypted information. To determine whether their argument will stand, one need only review the referenced section of the CCPA (Section 1798.50), which

Related People

Erika J. Gasaway

Partner

San Jose

408.299.1370

erika.gasaway@lathropgpm.com

Related Services

[Data Privacy &](#)

[Cybersecurity Compliance](#)

[Corporate & Business](#)

Related Sectors

[Retail & E-Commerce](#)

addresses security incidents and is the **only** section of the CCPA that gives way to a private right of action.

At the outset, it is important to understand that this right to bring a lawsuit is not unlimited, because the unauthorized access must pertain to certain specified types of unredacted or unencrypted information, *and* before an action can be filed, a defendant must be given an opportunity to cure the breach and the California Attorney General must be notified. The lawsuit alleges that the notice requirements were met.

The plaintiffs take the position that Zoom's failure to disclose to users that it shares personal information with Facebook constitutes a data breach because it is an unauthorized disclosure. While a matter of first impression, this position may push the boundaries of the data breach provision of CCPA beyond its plain language and intended scope. Even assuming that failing to notify users of these data sharing practices constitutes an unauthorized access, another key issue for the plaintiffs is that Facebook does not appear to have received from Zoom the type of personal information that falls within the purview of section 1798.50. In other words, even if the Zoom plaintiffs manage to convince the court that Zoom's data-sharing and lack of transparency constituted an "unauthorized access", the personal information at issue may be a non-starter.

A close look at Section 1798.150 suggests that only certain types of personal information, if subject to a breach, can form a basis for the limited private right of action:

1. An individual's first name or first initial and his or her 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:
 1. Social security number
 2. Driver's license number or California identification card number
 3. Account number, 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
 4. Medical information
 5. Health insurance information
2. A username or email address in combination with a password or security question and answer that would permit access to an online account.

The personal information listed in the complaint as being passed onto Facebook does not include any of the specific types of data listed in Section 1798.50, and should therefore arguably preclude a private right of action. As noted above, other than with respect to this limited right for certain security incidents, consumers have no private right of action for privacy violations *per se*, as also confirmed by Subsection (c) of 1798.150. As such, although this is a matter of first impression, the complaint appears to circumvent the plain language of CCPA in an attempt to "broaden" the limited private right of action.

Whatever the outcome for Zoom, this lawsuit is unquestionably an unwelcome distraction at a pivotal moment in Zoom's evolution. Moreover, this lawsuit raises the question as to what liability Facebook and other third parties could face for buying, receiving, and using the ill-gotten data allegedly provided by Zoom. Covered businesses that are purchasing data from data brokers and the like should investigate whether the data they are receiving and infusing into their sales and marketing channels is tainted by violations of the CCPA or other privacy laws. In addition, covered businesses that are monetizing their "influence" or market position by allowing third parties to collect and sell data from people who view their websites or purchase their products should investigate the methods of collection to ensure that California consumers are given the notice and opportunity to opt-out at the time of collection.



This class action lawsuit should serve as a strong wake-up call to covered businesses that have put off reviewing their privacy practices and/or compliance with CCPA and other applicable laws. Zoom has come under the microscope for various security and privacy violations, and while it had no choice but to publicly recognize some of its documented security issues, lawsuits such as this one – regardless of the merits – only add to the negative press. At the heart of this litigation is Zoom’s lack of transparency as to its data sharing practices, one of the key components of CCPA (and other stringent privacy laws such as GDPR). Despite the fact that the Zoom plaintiffs’ arguments do not fall squarely within the scope of the limited private right of action under CCPA, this is a matter of first impression: should they succeed in convincing the court to override the CCPA’s plain language, covered businesses should gear up for more class action litigation. One way to reduce the risk of any such litigation is to review your organization’s privacy and just-in-time notices, in order to ensure full transparency on the collection and disclosure of personal information.

If you have any questions please feel free to reach out to the data privacy attorneys at Lathrop GPM.