Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY

APRIL 9, 2020

Zooming In On Zoom's Security and Privacy Practices

With the outbreak of Coronavirus in the U.S., virtual meeting apps have seen an exponential increase in usage. From business meetings and remote real estate walk throughs, to online schooling to virtual happy hours—countless Americans have turned to these apps to replace their daily human interactions. Among the several apps that offer group-based virtual meetings, the Zoom app has undergone the most striking increase in popularity; going from its peak of 10 million users a day in December of last year, to 200 million users per day since the beginning of the pandemic.

But Zoom's rise in popularity has been accompanied by a storm of criticism regarding its security and privacy practices. Researchers have uncovered a number of flaws in its security. Some of these flaws have allowed uninvited attendees to break into and disrupt private meetings, a practice known as "Zoom-bombing." The *Washington Post* has also found that thousands of recordings of Zoom video calls had been left unprotected and viewable on the open web. The company has been forced to stop product development in order to focus on security and privacy enhancements.

As a practical matter, for those using Zoom for confidential business meetings, certain steps can be taken to increase the privacy and security of virtual meetings. For example, care should be taken to use a unique meeting ID and password for every Zoom meeting. If you have a weekly team meeting, do not use the same meeting ID weekly. Instead, generate a new one and require a new password each time. Also, consider using some of the other controls available in the Zoom app, such as the "Waiting Room" feature, which allows an administrator to control who is permitted to join a Zoom meeting. While these steps are not fail-proof, they provide a heightened level of security and will decrease the likelihood of Zoom-bombing, or other uninvited attendees joining Zoom meetings.

With respect to its privacy practices, Zoom has also run into some recent difficulty. Zoom now faces two class action lawsuits for one particular privacy practice: Until late March of this year, the Zoom iOS app was sending certain user information to Facebook every time a Zoom user opened the app. The Zoom iOS app's leakage of user information to Facebook was revealed on March 26, when *Motherboard*—the online magazine and video channel owned by Vice Media—published the results of its investigation of Zoom's privacy practices. According to *Motherboard,* Zoom's iOS app routinely transmitted user-specific data to Facebook whenever the app was launched, including users' IP addresses and unique information about the specific device which the user was using for Zoom meetings. A day later, Zoom acknowledged that its iOS app was transmitting data to Facebook as part of the app's usage of the "Login with Facebook" feature of Facebook's Software Development Kit (SDK) and updated its iOS app to stop using the Facebook SDK. While Zoom has acknowledged that certain information was being sent to Facebook, Zoom claimed that that the transmitted information did not include the names of meeting attendees or information relating to the content of virtual meetings, such as meeting notes.

Three days later, a Zoom user filed a class action against Zoom in U.S. District Court in the Northern District of California. *See Cullen v. Zoom Video Communications, Inc.,* 20 Civ. 2155 (N.D. Cal. March 30, 2020). A day later, a second class action was filed, also in the Northern District of California. *See Taylor v. Zoom Video Communications, Inc.,* 20 Civ. 2170 (N.D. Cal. March 31, 2020). The complaints assert a variety of theories of liability for Zoom's disclosure of user information to Facebook. Notably, both complaints allege that Zoom violated California's recently-enacted California Consumer Privacy Act (the CCPA), when it failed to properly notify its users that it was transmitting user-specific information to Facebook.

These two lawsuits will provide the courts an early opportunity to interpret the CCPA, which went into effect January 1, 2020. The CCPA significantly expanded the data privacy rights of California residents. Among other things, the CCPA gives consumers the right to know what personal information a covered business has collected about them, its source and the purpose for which it is being used. Unlike Europe's General Data Protection Regulation (GDPR), the CCPA does not require consumers to "opt in" for the sale or use of their personal information. Rather, the CCPA requires specific privacy notices regarding the information collected and further requires covered businesses to provide the ability to opt out of the sale or use of personal information.

For businesses that collect the personal information of California residents, stay tuned. Zoom may be one of the first companies to draw scrutiny under the CCPA; it will certainly not be the last.

If you have any questions about this Information Memo, please contact John D. Clopper, Jessica L. Copeland, any of the attorneys in the Cybersecurity and Data Privacy or the Litigation Practice Groups or the attorney in the firm with whom you are regularly in contact.

BOND SCHOENECK & KING ATTORNEYS