MSF CLIENT ALERT

Meister Seelig & Fein LLP | 125 Park Avenue New York, NY 10017 | 212.655.3500 | meisterseelig.com

Video Conferencing Privacy and Security Alert

Zoom has been under fire for its privacy and data security practices this week as the FBI issued warnings about using the platform, the New York Attorney General pressed for accountability and transparency, and a class action lawsuit was filed in California against the video conferencing technology company.

As the workforce increasingly turns to telework to maintain business continuity, and as universities and schools across the country begin to rely on distance learning during the COVID-19 crisis, an increasing number of users have begun to deploy Zoom. Zoom does not appear to be ready for the spotlight.

In addition to reports that the service lacks end-to-end encryption and is sharing user (and non-user) data with Facebook, Zoom seems unable to adequately address increases in unauthorized access to private Zoom videoconferences, now called "zoombombings". In Massachusetts, for example, a teacher reported that someone entered a Zoom virtual classroom, shouted a profanity, and disclosed the teacher's home address to those in attendance.

Moreover, while Zoom is at the center of attention for the moment, these issues are likely to transcend platforms. Other popular videoconferencing solutions, including Google Classroom, Microsoft Teams, House Party, Zearn, Seesaw, Padlet, Razzkids, Epic, and Canvas, to name a few, may have similar vulnerabilities.

Businesses, customers, clients, teachers, parents, friends and families wonder what may be happening in the background as they come to rely on video conferencing applications for business continuity, livelihoods, education and basic human interaction. As a result, we can expect to see increased regulatory and law enforcement scrutiny, as well as more lawsuits alleging breaches of privacy and data security laws, consumer protection laws and unfair competition laws.

Guidance for New York Businesses

The New York SHIELD Act, signed into law on July 25, 2019, applies to any person or business that owns or licenses private information of a New York resident. The SHIELD Act provides specific safeguards for the collection, storage and disposal of private information of New York residents, an expanded definition of "private information," data security protection requirements, and notification requirements in the event private information is viewed, communicated, used or altered by someone without authorization.

The SHIELD Act requires businesses to develop, implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information of New York residents, setting forth specific criterion for developing a data security program with reasonable administrative, technical and physical safeguards. Read more about the SHIELD Act requirements in our October 20, 2019 Client Alert https://www.meisterseelig.com/2134-2/

While there is no private right of action, the New York Attorney General may bring claims against companies and individuals who fail to comply with the law to enjoin the alleged activity and assess civil penalties under the New York Consumer protection laws, which provides damages of up to $5,000 per violation.

The New York Attorney General wrote to Zoom on Monday, March 30, 2020, to express concern about Zoom's capability to keep up with the extraordinary increase in traffic it was seeing as a result of the COVID-crisis teleworking and distance education mandates. Specifically, the New York Attorney General inquired about the following:

- What, if any, new security measures Zoom has put in place to handle increased traffic on its network and to detect hackers.
- Citing reports that Zoom shared user and non-user data with Facebook, the office asked for information on the categories of data Zoom collects, as well as the purpose of any data sharing and the identities of entities to whom Zoom provides consumer data.
- Zoom's policy for obtaining and verifying consent in primary and secondary schools, as well as description of third parties that received data related to children.
- Details about any changes the company put in place after a security researcher exposed a flaw allowing hackers to take over Zoom webcams.

The Attorney General's letter appears to acknowledge that Zoom has implemented some measures to respond to data privacy and security issues as they have arisen. However, it is a clear signal that regulators will require a better understanding of the internal workings of Zoom and other video conference and technology platforms to ensure that the providers of such solutions are complying with privacy and data security laws in these trying times.

All businesses, particularly those seeing an uptick of users during the COVID-19 pandemic, should review their privacy policies immediately to ensure the policy is clear and compliant with applicable laws, including rules that require accurate disclosure of the types of information collected, how the information is collected, what the information is used for, and whether it is sold or shared with third parties. In some states, businesses may be required to include a description of the user's disclosure, access, opt-out mechanisms and nondiscrimination rights. Businesses should also ensure their telework policy or guide addresses requirements for physical and information security.

Companies based in New York may be subject to privacy and data security laws of other states, including California's Consumer Privacy Act (CCPA), and potentially international privacy and data security laws and regulations such as the General Data Protection Regulation (GDPR). If the business provides services to schools and children, there may be additional state and federal laws and regulations such as the Children's Online Privacy Protection Act (COPPA). As such, businesses will need to ensure that the company's privacy policies, notices and practices are in compliance with these laws and regulations, as well as those of New York.

Guidance for Users

Whether you are using video conferencing platforms for business, education or personal reasons, it is important to review and understand the privacy policies of the services being used to better understand the types of personal information that is being collected and how that

personal information is used, managed and shared. Some states, such as California, provide more disclosure, access and opt-out requirements than others.

Also review the service provider's features to see if there are privacy and security settings that you can engage to better protect your personal information and the information exchanged by you and your meeting participants while using the video conferencing platform.

Monitor webcam access. Ensure that you leave the meeting and close the video conferencing platform when the meeting has concluded. Consider purchasing a camera cover or using a piece of opaque tape to cover built in cameras on your laptop or personal device when you are not using the webcam.

If you are hosting a meeting, do not (1) enable settings to make the meeting public, or (2) publicly post the meeting access information (e.g. weblink, pins, etc.); instead email this information directly to your meeting participants. If using Zoom, consider controlling your participants further by using Zoom's waiting room feature, which permits the host to admit participants on a more controlled basis.

Note that although conference hosts can record the meetings, there will be a "Recording" icon that appears on the participant's screen that will alert you to that the meeting is being recorded. If you are concerned that the meeting is being recorded you can choose not to participate in the meeting, raise your concern to the host through the video or chat feature and perhaps the host will cease recording, or continue to participate but be aware that your conversation and video are being recorded.

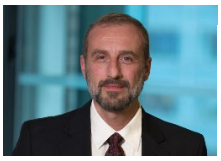
If you are using a video conferencing platform for work, be sure to review and comply with your employer's telework policy or guide addresses requirements for physical and information security and comply with the requirements.

Furthermore, the FBI advises the following specifically with regard to using Zoom:

- Do not make meetings or classrooms public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.
- Manage screensharing options. In Zoom, change screensharing to "Host Only."
- Ensure users are using the updated version of remote access/meeting applications. In January 2020, Zoom updated their software. In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join.

See the complete FBI advisory here: https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

Let Us Know How We Can Help



Antonio Papageorgiou
Partner | Chair, Intellectual Property
(212) 682-9003 | ap@msf-law.com

Katherine E Lewis
Partner, Intellectual Property |
Director of Innovative Ventures
(646) 539-3730 | kel@msf-law.com