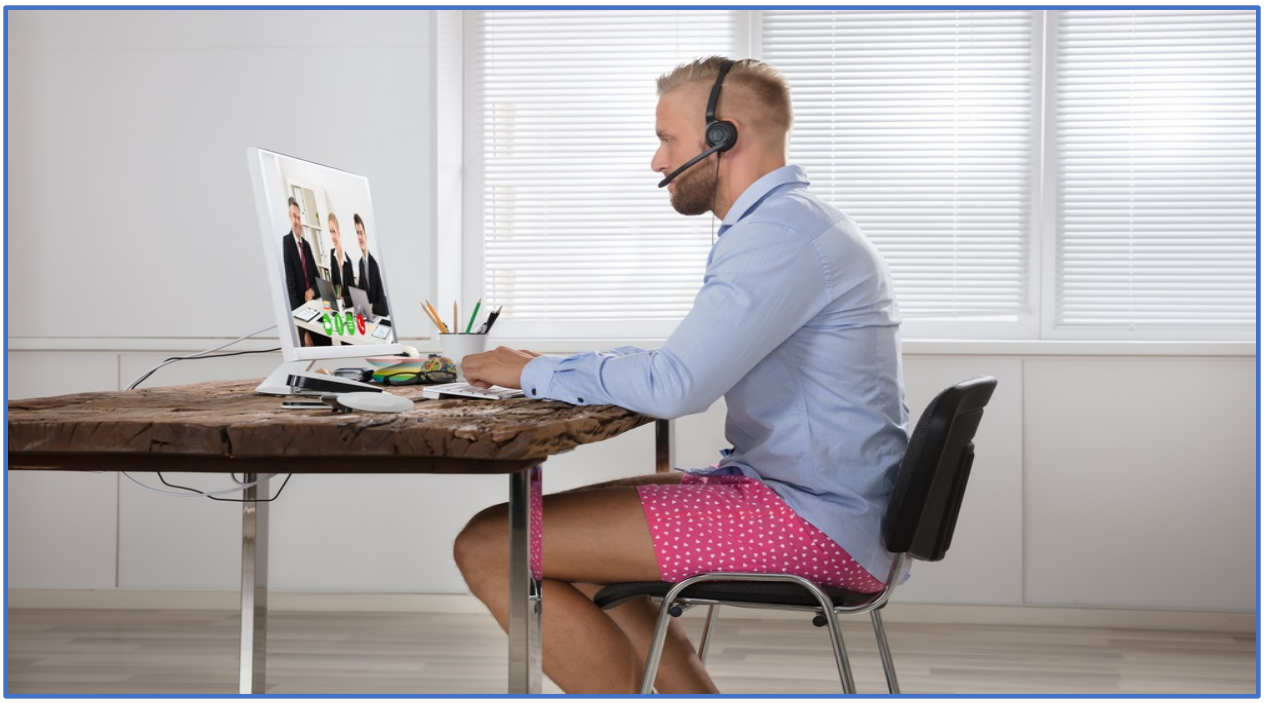
Zoom Training for Lawyers – and Using it Securely



State Bar of Michigan

May 26, 2021

Presenters: Sharon D. Nelson, Esq. and John W. Simek
President and Vice President, Sensei Enterprises, Inc.
jsimek@senseient.com; snelson@senseient.com
https://senseient.com; 703-359-0700

Zoom Training for Lawyers - and Using it Securely

Updated December 1, 2020

by Sharon D. Nelson, Esq. and John W. Simek

The coronavirus pandemic has forced a lot of lawyers to utilize video conferencing to "meet" with co-workers and clients. One of the most popular video conferencing platforms is Zoom. There are others, but we see Zoom as the choice of many lawyers, especially those in solo and small firms. Many courts are also using Zoom for various court proceedings. While we can't cover all the options and settings for Zoom (there are a ton of them), we'll try to give our advice on the best way to use and secure Zoom for your firm.

The growth in Zoom usage has exploded. As of the end of December 2019, there were approximately 10 million free and paid daily meeting participants. In contrast, that number has increased to over 300 million free and paid daily meeting participants in April of 2020. The boom in usage has squarely put the crosshairs on Zoom. Multiple security and privacy issues were discovered and exposed by security researchers and journalists. Some of the publicity was justified and some of the media statements were wrong or overblown.

On April 1, 2020, Zoom CEO Eric Yuan announced that there would be a feature freeze for the next 90 days while resources are concentrated on fixing the "biggest trust, safety, and privacy issues." As a result, we continue to update our previous Zoom article(s) as Zoom was in damage control mode fixing those issues. Make no mistake about it though – clients and lawyers both love Zoom and, as Zoom has fixed more and more security defects, we believe it is a darn good videoconferencing solution for lawyers as long as they learn how to use it properly. Besides the security improvements, Zoom is constantly enhancing and adding features, which is another reason we continue to provide updates to the article(s).

Now that the 90 day "moratorium" feature freeze is over, the latest Zoom version includes features to enhance the user experience. We'll address a few of the new features lawyers will want to know about later in this document.

Basics

The first question for rookies is…what the heck is this thing called Zoom? According to the website, "Zoom is the leader in modern enterprise video communications, with an easy, reliable cloud platform for video and audio conferencing, collaboration, chat, and webinars across mobile devices, desktops, telephones, and room systems. Zoom Rooms is the original software-based conference room solution used around the world in board, conference, huddle, and training rooms, as well as executive offices and classrooms."

Zoom is extremely easy to use (for lawyers and clients!) and is available across multiple platforms and operating systems. You can use your mobile device with apps available for

Android and iOS. There are desktop clients available for macOS, Windows and a bunch of Linux/Unix versions (e.g. Ubuntu, Linux, CentOS, OpenSUSE, etc.).

Equipment

To state the obvious, you will need some sort of camera to participate in a video conference call. Most modern-day laptops are equipped with a webcam for video calls. You could even use your iPad or smartphone with Zoom. Another consideration is sound. The built-in microphones for laptops or phones may not sound particularly good if you are on the receiving end. Consider using a headset (with microphone) or earbuds. You'll be able to hear better, and so will all the other participants. Besides sounding better, headsets and earbuds help cut down on the ambient noise as well as keeping one side of the conversation private. Family members may be able to hear your side of the discussion (you really should be in an isolated room/area to minimize that), but they won't be able to hear the other participants.

If you are using your home desktop computer to participate in a video conference session, you will probably need some sort of camera and microphone device to facilitate the video transmission. As a result of the pandemic, besides a shortage of toilet paper and hand sanitizer, there was also a shortage of available webcams. To add a webcam to your desktop computer, we would suggest investigating several of the models from Logitech. The model C920, C920S, C922 or C930E are all good models to add to your computer setup. The referenced models connect via USB and provide 1080p video resolution and stereo sound. You can also add a webcam to your laptop if it is not equipped with video. The good news is that many of the Logitech models are back in stock. In addition, Amazon has several models that can be substituted. We would recommend considering a camera/microphone combination capable of 1080p resolution, wide angle and supporting a tripod mount.

Don't forget where you physically sit during the video conference. If your back is to an open window, the brightness may make you difficult to see. Light sources (lamps, skylights, etc.) behind you will have the same effect. Objects behind you may be distracting too. Think about what the person on the other end is seeing. Be cognizant of those around you. Family members may be able to hear you discussing confidential information even if you are wearing a headset as we've discussed above.

Participating in a Meeting

We've participated in a slew of Zoom meetings over the years, but it sure feels like we're now involved in one or two a day instead of one every several months. It seems obvious to us that you need to be in physical possession of the device you use to participate in a Zoom meeting. Apparently, a lot of attorneys don't get the obvious or haven't completely thought things through.

Many of us are still working from home and may be remotely connecting to our computers at the office. If so, you'll need to **NOT** remotely connect and must use your home computer, smartphone, iPad or some other device that you physically possess. If you try to participate in a

Zoom meeting while remotely connecting to your office machine, it will be just as if you were sitting at your office desk. We can't tell you the number of times we were looking at an empty desk chair. You are not sitting in your office so participants can't hear you either. In other words, when you remotely connect to your office computer, Zoom uses the microphone and camera of that office machine. It seems silly, but invariably there's at least one participant in a Zoom meeting that remotely connects to their office computer and wonders why we can't see or hear them. Good thing there is a chat function in Zoom.

All you need to do is have some way to access the meeting invite details from a physical device you have control over and which is in your possession. If the invite went to your firm's email address, just access it from your smartphone (assuming you can get to your firm email from your phone); otherwise, just forward the message to a personal email account you can access from your home machine or other personal device. Remember…when participating in a Zoom meeting, the video camera must be able to "see" you and the microphone must be able to "hear" you. When you're at home, your office machine can't do that.

We've also had experience where we couldn't hear a participant, yet they were unmuted in Zoom. The likely cause is that the microphone is muted on the actual device they are using or the wrong microphone is selected. The method to checking if your computer microphone is muted varies by computer manufacturer and model. Bottom line…check to make sure the microphone/sound is not muted on your physical device. That even applies if you use a headset. Most wired headsets will have some type of switch assembly in the cable to adjust volume and mute the microphone. Apparently, inadvertently bumping up against the microphone mute button is common.

Meeting Management

While you are in a meeting, clicking the Participants icon in the bottom menu bar pops a panel to the right that shows all the participants for the meeting. You can see the status of the user's microphone (muted or unmuted) and status of their video camera. Obviously, there will be no camera icon if the participant dialed in with a phone number. The participants panel is where the host can manage and control the participants. The host can 'mute all' or mute participants individually. The host has other options as well such as changing the name of the participant, stopping their video, preventing screen sharing and requesting a participant to start their video. The host can also remove a participant, send them to the waiting room, make them a co-host, etc.

Recent updates of the Zoom client have changed the way muting control works for the host and participants. Even though the host can mute an individual or mute everyone at once, unmuting is left to the participant. The host can no longer unmute a participant without their approval. The host can request to unmute a single participant or request to unmute all. The participant then receives a pop-up message asking for approval to be unmuted. Many users have expressed frustration with this change in unmuting operation. Perhaps to placate users, Zoom has modified the unmuting process yet again to allow the participant to approve all future unmuting requests from the specific host. In other words, if you participate in a lot of meetings

with the same host, you can allow the host to unmute you without the typical request box coming up for all future meetings.

When you click on a meeting link, you will be prompted to open the Zoom application. The default view shows the participants across the top bar with the speaker showing in the center panel. This is called speaker view. If someone else starts talking, the video will shift to that speaker. If have more than a handful of participants, it is difficult to see who is in the meeting. Taking your mouse to the upper right corner of the screen will give you the option to change the view to gallery. The gallery view shows all participants in their own "square" with the speaker's box having a yellow outline. The outline will bounce around to the various speakers and is less annoying than the speaker's video constantly being switched out. Think of the view as being similar to the introduction of the Brady Bunch TV show or the TV game show Hollywood Squares, where each person was in their own "box." Many new Zoom users have no clue about how they can change the view to "gallery." That is something we have to explain in most meetings.

Zoom's popularity hasn't gone unnoticed by the competition either. Zoom's gallery view is very popular. So much so that Microsoft and Google have since implemented their versions of a grid view. Zoom can display up to 49 participants in gallery view on a single screen. You're going to need a pretty big monitor or hook up to your big screen TV in order to see that many people clearly. Google has released an update to Meet that can display only up to 16 people simultaneously. Microsoft Teams supports nine people in a gallery view, which is a far cry from 49. The Education version of Teams does support a 49 participant view similar to Zoom called Large Gallery view. It seems like Zoom has won the gallery view battle for now.

Zoom released an update some time ago that is most visible to those hosting meetings. There is now a new Security icon in the lower menu that replaces the Invite button. The icon allows the host to quickly and easily find and enable/disable security features. When you click the icon, hosts and co-hosts will be able to lock the meeting, remove participants, restrict a participant's ability to perform some actions (rename themselves, share screens, etc.) and enable the Waiting Room even if it's not already enabled.

Features

The primary function of Zoom is to facilitate video conferencing. It supports video and audio transmission for each connected user over the internet. There's also a dial-in number for audio only connections. Some people use Zoom as an audio conference bridge so that users won't have to incur potential long-distance phone charges.

You can also configure Zoom to allow file transfers and screen sharing. Screen sharing is very common when observing a product demo. It is even used when giving CLEs using Zoom. The presenter can mute all the attendees and share their PowerPoint slides from their computer desktop. There is also a whiteboard feature which participants can annotate for all to see.

There are a lot of meeting controls available to the host. As an example, you can control the audio of the participants. All participants can be muted when they first join the meeting. Audible tones can “announce” the joining of a participant. Sessions can be recorded in the cloud or locally to a user’s computer.

Another helpful feature for mediators is the Breakout Room feature, which is disabled by default. You create the rooms and then assign participants to a specific room. You even have the option to preassign participants to specific breakout rooms when you first schedule the meeting. In addition, Zoom now allows participants to self-select which breakout room they would like to join. Obviously, you would not enable that capability for mediations or other host-controlled events. When the host opens the breakout rooms, each participant gets a notice to move to the room. Each room is isolated from the others, just like you would be in a real mediation. The participants can take advantage of the Zoom features (e.g. screen share, chat, etc.) among everyone in the room. The host can freely move among the breakout rooms. If there are co-hosts, the host can move them among the various rooms as needed. When the host closes the breakout rooms, the participants get a notice that the room will close in a certain amount of time and need to return to the main meeting space. Of course the mediator should be the one that hosts the meeting. We would not recommend allowing one of the parties to be the host in a mediation unless separate Zoom meetings were created for the appropriate participants, which would ensure separation of the parties. The disadvantage with separate meetings is that you can’t easily move among the various rooms as you would in a real physical mediation. Besides mediations, the Breakout Room feature is useful for depositions as well.

Apparently, the breakout room feature has gotten the attention of Cisco. Cisco Webex now has a feature it calls Side Rooms to compete with Zoom’s Breakout Room feature.

You can record Zoom meetings too. The paid subscriptions offer local and cloud recording. The Pro plan includes 1GB of cloud recording storage. You can add more storage space for an additional fee. We would highly recommend not recording to the cloud. Cloud recording means Zoom stores the recording and manages it. Local recording means you have control over the distribution of and access to the recording. One downside is that local recording is not available in the iOS or Android app. You must use a computer to be able to record locally. Another concern is the issue of encryption. Encryption is not possible for the recorded information. The good news is that local recording is only available for the host unless the host allows participants to record locally.

We are asked how the recordings are handled when you are using breakout rooms, especially if used for mediations. If you elect to do cloud recording, only the main room is recorded. The breakout rooms are not recorded. Local recordings are done for whatever room the host is in. That would typically mean the main meeting room, but a breakout room would be recorded if the host (mediator in our example) went into one of the breakout rooms. The host always has the option to stop the recording and then go into the breakout room to prevent recording the

breakout room session. The host could then resume the recording once they exit the breakout room and return to the main room.

When configuring Zoom, do not enable the cloud settings or automatically record. It is possible to record without the host, but we would recommend against it. Prior to initiating a local recording, make sure the option is enabled. Login to your account from a browser and go to Settings and then the Recording tab. Make sure the "Allow hosts and participants to record the meeting to a local file" is enabled. You can also configure the host to allow the participants to record locally. To start a recording, click on the Record button in the bottom menu. Select the "Record on this computer" choice. The host and participants will see a visual indicator in the upper left to indicate that recording is in progress. A visual indicator will also appear in the participants panel if one of the participants has initiated a recording. There will be an audio notification too if you have configured it, which we highly recommend. You can stop or pause the recording at any time during the meeting. Once the meeting is over, the recording will get converted and downloaded to your computer. The host needs to stay connected to the internet during the entire download process. The default location to save the recording is in the Zoom folder in the host user's Documents folder.

Another best practice is to close the meeting once all the intended participants have joined. You do this by selecting "Manage Participants" icon in the bottom menu and then click "More" at the bottom of the panel or by clicking the new Security icon. Select the "Lock Meeting" to prevent anybody else from joining. As you can see, the intent is to create as many barriers as possible to prevent unintended attendance to your meeting. So-called "trolls" having a way of joining for mischievous reasons, including Zoom-bombing with inappropriate content, without those barriers.

Video Filters

As previously mentioned, the Zoom feature freeze is now over. One of the new features introduced with version 5.2.0 of the Zoom client is video filters, which are enabled by default. Video filters are configured in the Zoom app and allow the user to "alter the look of their video with color grading, foreground and frame filters." The setting is now called Background & Filters in the app. If you select Background & Filters, there are now tabs for Virtual Backgrounds and Video Filters. You can select a particular video effect such as being framed in an analog TV, picture frame, a theater scene, etc. If you want to get a little crazy, there are video filters to wear a pirate patch, pizza party hat, a graduation cap and multiple other effects. While video filters can lighten the mood for your video conference, it isn't very professional to use a filter for communicating with clients and colleagues.

Technical Adjustments

Another new feature is the ability to adjust video brightness. This is a great way to improve your appearance if your light conditions are less than optimal in low light situations. Go to Settings and select Video. There is now an option called "Adjust for low light" under the My

Video section (not enabled by default). If you check the box, you have the option to automatically adjust the brightness of your video or manually with a slider.

Another added feature is improved background noise suppression. Under the Audio section in the app Settings is "Suppress background noise." The default setting will be Auto. You can override the Auto setting and select Low, Medium or High. At the low setting, background music can complement your meeting. Using the High setting can provide distraction-free audio. We would recommend using the High setting for important meetings or court appearances using Zoom. The last thing you need is to hear is a dog barking, kids screaming or loud lawn mowers in the background as you are making closing arguments.

Cost

There is a free version of Zoom, but there is a 40-minute limit per meeting that has three or more participants. The Pro version is the most popular for solo and small firm attorneys. The cost is $14.99/month per host account. (The host is the one who schedules the meeting.) Each session is limited to 24 hours (don't invite us if you go that long) and you can have up to 100 participants. There are additional admin controls as well. If you pay annually, the cost is $149.90 ($12.49/month). The next level up is the Business subscription, which is $19.99/month per host and requires a minimum of 10 hosts. There are a lot of enterprise features available with the Business plan such as a vanity URL and the ability for on-premise deployment.

We're confident the Pro plan is more than adequate for most law firms. If you need more than one host, just purchase an additional Pro plan subscription.

Configuration Settings

We're not going to go through all the various ways you can use or control Zoom. Assuming you have purchased a Zoom subscription, we will make some suggestions for configuring and using Zoom in a more secure fashion. First, make sure you are using the most up-to-date version of Zoom. If you have previously used Zoom, you probably already have Zoom installed. To manually download the latest version, launch the Zoom application, log in to Zoom and click on your user icon in the upper right (it probably has your initials or your profile picture). Select "Check for Updates" and follow the instructions. Periodically check your configuration settings after updating. We have experienced some of our configuration settings getting changed back to defaults after an update. We would recommend checking your configuration settings at least once a month.

Consider checking some of the default settings prior to scheduling the meeting. The first one is screen sharing. The default is now set to allow only screen sharing by the host. Make sure the setting is **not** configured to allow all participants to screen share. That means anyone can share their screen with inappropriate content. Yes, even bizarre sexual content. You can always change the setting during a meeting to allow those other than the host to share their screen if needed, but make sure the default is set so that only the host has screen sharing enabled.

The online Zoom bond hearing for the 17-year old teen accused of the July 15 attack on Twitter and tweeting a bitcoin scam for the Twitter accounts of high-profile users was "Zoom bombed" with pornography for about 15 seconds. We are suspicious that screen sharing was allowed for all participants, which is **not** a default setting. User error strikes again.

Another default setting is to require a meeting password. You can configure Zoom to include the password in the meeting invite or you can distribute the password separately. A related default password setting is to require a password for those joining by phone as well. As a security measure, passwords are now required for all meetings including those using your Personal Meeting ID. Even though it is now the default, check your settings to make sure passwords are required for all participants, including those just using a telephone.

It would be nice if everyone in the meeting used their video cameras so you could verify who they are. However, some participants may not want their cameras turned on or they call in using a telephone. There is another Zoom setting to prevent someone from changing their display name to indicate they are someone else. When you are in the meeting, go back to the managing participants panel and click on "More" again. Make sure that the "Allow Participants to Rename Themselves" is unchecked.

An additional step to prevent the display of inappropriate content is disabling virtual backgrounds. Go to the "Setting" section in Zoom and select the "In Meeting (Advanced)" choice. Disable the "Virtual background" option. This will prevent someone from displaying an inappropriate image or video as their background. Having said that, you may consider allowing participants to utilize virtual backgrounds. Virtual backgrounds are useful to "hide" the clutter of your surroundings or to show a pleasant scene. We would suggest leaving virtual backgrounds enabled unless you experience abuse. If you are particularly paranoid, disable them.

However, you may want to leave virtual backgrounds enabled, especially if you want to take advantage of a new feature available in version 5.2.0 of the Zoom client. Even though the feature is in beta, you can now share PowerPoint as a virtual background. Your video will overlay the PowerPoint slides similar to the weathercaster style that we've all seen on TV. Using a green screen will maximize the effect and make your background "disappear," only leaving your image superimposed on your PowerPoint slide. The option is under Share Screen in the advanced options. Once you select your PowerPoint file, you use the arrow keys at the bottom of the screen to advance the slides and change your background. The viewer and presenter need to have the version 5.2.0 client or later installed to take advantage of the feature. This new feature could be very effective during opening or closing argument, assuming the court allows you to show PowerPoint slides.

Control when the meeting starts. Don't let the participants join the meeting before you do. Who knows what could be going on before you connect? After all, it is your meeting. In the "Schedule Meeting" section of "Settings," make sure the "Allow participants to join anytime" option is disabled, which is now the default. An alternate control mechanism is the Waiting

Room feature, which is now turned on by default. Participants connecting prior to the host are held in the waiting room. The host then admits the participants individually or all at once. Enabling the Waiting Room feature automatically disables the “Allow participants to join anytime” option.

As a host, you may find it is overkill to review each attendee in the waiting room prior to starting the meeting. Changing your configuration to disable both the waiting room and “Allow participants to join before host” may be good enough to control entry to the meeting. You can always set the Waiting Room option on an individual meeting basis. The Waiting Room is a good feature to use if you anticipate many participants and the meeting link is made public. It’s also a good way to have a quick conversation with someone prior to starting a meeting. As an example, perhaps you scheduled a meeting to discuss a potential settlement with an opposing party. As participants are queuing up in the Waiting Room, you could allow your client and associate to enter the meeting for a quick chat prior to allowing all participants to enter.

If you are particularly paranoid about what someone might pop up or write on a screen, you should turn off annotations and whiteboard in the “In Meeting (Basic)” section.

Two other settings to disable deal with the user experience at the end of the meeting. We find it particularly annoying to have survey questions or ratings appear after visiting a site or at the end of a webinar, etc. Be nice to your participants and turn off the Feedback to Zoom and Display end-of-meeting experience feedback survey settings. They are both enabled by default.

Scheduling

It is highly recommended NOT to use your Personal Meeting ID (PMI) when scheduling meetings. Your PMI is a constant value and never changes unless you manually edit it. Once it is known to someone else, they could connect to the meeting whether they have been invited or not. Of course, requiring a password for PMI meetings will help, but our recommendation is to not use PMI - period. Allowing Zoom to automatically generate the meeting ID is a more secure option. This means that each scheduled meeting will have a unique random meeting ID. This greatly enhances the security of using Zoom.

Another available security setting when scheduling a meeting is to require registration. You must have a paid Zoom subscription to require meeting registrations. Meeting registration means the participants register with their email address, name and questions. There are some predefined questions such as Phone, Industry, Job Title, Address, etc. You can also create your own custom questions. The registration option is not available in the Zoom app when scheduling meetings. You must schedule your meeting using a web browser in order to select the Registration Required option. The default is to automatically approve all participants after they complete the registration. You may want to change the setting to manually approve participants for the meeting. After registration is approved (manually or automatic), the participant will receive information on how to join the meeting. Meeting registration is another good way to further restrict meeting participants and help prevent Zoom-bombing.

Account Security

Just like any other service you use, your password should be strong and not easily guessed. In addition, two-factor authentication (2FA) should be enabled for the account. It still amazes us that the default is not set to require 2FA. You enable 2FA for your Zoom account by selecting "Security" in the "Admin" section, under "Advanced." Turn on the "Sign in with Two-Factor Authentication" option. Unlike most implementations of 2FA, you will have to enter the code every time you login. There is currently no option to trust the device you are using for any period of time.

Video Conference Etiquette

When you are participating in a Zoom meeting, mute yourself so that other participants don't hear all your background noise and potential disruptions. Barking dogs, ringing doorbells, children screaming, etc. do not leave a very professional impression. Unmute yourself when you have something to say. A very fast way to temporarily unmute yourself is to press and hold the space bar. Just like the old-style push-to-talk microphones, holding down the space bar unmutes and allows you to be heard. Releasing the space bar mutes you again. While we're at it, become familiar with hotkeys and keyboard shortcuts for Zoom. There are a lot of them. Zoom has a help article that discusses hotkeys and keyboard shortcuts for the various operating systems. https://support.zoom.us/hc/en-us/articles/205683899-Hot-Keys-and-Keyboard-Shortcuts-for-Zoom

Another etiquette consideration is positioning of your video camera. If you have a separate USB webcam, position it at face level pointed directly at you. If you use the webcam in your laptop, make sure the laptop is elevated to have a straight view of your face. Set your laptop on a few books to get it higher if needed. The last thing you want is the camera looking upward exposing your nostrils. Not pretty.

Meeting Disruptions

The unfortunate thing is that Zoom-bombing and meeting disruptions are continuing to plague us all. Even our daughter-in-law recently experienced an unfortunate Zoom meeting where uninvited participants registered for a meeting where the registration link was made public. Registration was automatically approved, thereby giving the unintended participants access to the meeting credentials. There are far worse examples of Zoom meeting abuse. We've already covered several suggestions for controlling who attends your meetings and how to restrict participant capabilities.

To help combat any potential meeting abuse, Zoom has released some new security enhancements. Remember the Security icon where Zoom puts all security related features in one place? Well, there is now a "Suspend Participant Activities" choice under the Security icon available to the hosts and co-hosts. If you have an unintended or disruptive participant, just click on the selection to pause the meeting to remove the participant. When you click on the "Suspend Participant Activities" option, all video, audio, annotation, screen sharing, recording and in-meeting chat will stop. In addition, the Breakout Rooms will end. Once the meeting is

suspended, the host or co-host will have the opportunity to report the user, share any details and optionally include a screenshot. Once they click on “Submit”, the reported user is removed, and a notification is sent to the Zoom Trust & Safety team. The meeting can then be resumed, but you have to re-enable each of the disabled features that you would like to use. The feature to Suspend Participant Activities is enabled by default. You have always had the ability to report users from the security icon, but now you can enable the reporting for all meeting participants.

Zoom is also trying to help cut down on the abuse by releasing an At-Risk Meeting Notifier. The service scans websites and public social media searching for publicly shared Zoom Meeting links. The tool attempts to determine if a meeting looks to be at high risk of being disrupted and will alert the account holder via email with suggestions on what to do. The suggestions may include scheduling a new meeting after deleting the at-risk one, enabling additional security options or using another Zoom service.

Privacy

It’s rare that we come across an attorney that has read the Terms of Service, Acceptable Use or Privacy Policy. The Terms of Service for Zoom is seven pages and was updated on April 13, 2020, probably as a result of the COVID-19 pandemic. Zoom’s Acceptable Use Policy is only two pages and was updated on July 6, 2020. Finally, Zoom’s Privacy Statement is ten pages and last updated in August 2020. You should thoroughly read the Privacy Statement to see all the data that Zoom collects and how it uses the data.

Bottom line…Zoom collects a lot of data from users about their devices, activities and data shared/transferred. Consumer Reports pointed out that advertising campaigns could be developed from the videos and chat messages. Like Facebook, Zoom could use facial recognition technology against all the recorded videos. To be fair, Zoom has clarified and changed some of its past practices. As an example, Zoom removed the Facebook SDK (Software Development Kit) in the iOS client and reconfigured it to prevent unnecessary collection of device information. Previously, Zoom would send data about participants and used LinkedIn to match people. If a participant had a LinkedIn Sale Navigator account, they could access the other participants LinkedIn details without the participant knowing. Zoom has since disabled the feature.

A major difference between Zoom and its competition is the amount of control hosts have over participants and their activities. We’ve already discussed some of the recommended configuration settings to restrict what participants can do. Director of privacy and technology policy at Consumer Reports, Justin Brookman, said, “Zoom puts a lot of power in the hands of the meeting hosts. The host has more power to record and monitor the call than you might realize if you’re just a participant, especially if he or she has a corporate account.”

Citizen Lab discovered that some participant traffic was being rerouted through servers in China. As it turns out, Zoom uses geofencing to control traffic flow. Participants outside of China do not route through China and those in China stay within servers in China. When network traffic started to increase significantly, additional servers were added to Zoom’s

network. Unfortunately, a mistake was made and servers in China were improperly added. Therefore, some traffic was routed through China when it shouldn't have. After the report by Citizen Lab, Zoom removed the errant servers from the traffic flow.

Besides removing the improperly configured servers, Zoom released an update that allows for even greater control of network traffic. If you have a paid subscription, you can now control which servers have the ability to handle your network traffic. Go to the In Meeting (Advanced) section of the Settings. Find the section where you can define the data center regions for your meetings/webinars. By default, all of the regions are selected. The available regions are data centers located in Australia, Brazil, Canada, China, Germany, Hong Kong SAR, India, Ireland, Japan, Netherlands, Singapore, and United States. Uncheck any region where you don't want traffic to flow through. Unchecking a region may cause trouble for those participants that are calling in with a phone number from that region. We have our account configured to allow only data centers located in the United States to handle our Zoom traffic. You always have the option to override your default traffic setting and select additional regions on a per meeting basis. As an example, we will designate Canada and the United States if we are scheduling a meeting where our Canadian friends will be joining.

Encryption

Security of Zoom meetings is a major concern of millions of users. Some companies and agencies have banned the usage of Zoom. Some companies are asking their employees not to use Zoom but haven't banned it outright. Some think that competing products are more secure and should be used instead. We believe the truth is somewhere in between. Several months ago, Zoom clarified their architecture and encryption schemes. The major criticism was the lack of end-to-end (E2EE) encryption despite Zoom's earlier claims. Zoom was using the term end-to-end encryption in a way that is not the commonly accepted definition. Busted.

Zoom explained its encryption in a blog post on April 1, 2020. "To be clear, in a meeting where all of the participants are using Zoom clients, and the meeting is not being recorded, we encrypt all video, audio, screen sharing, and chat content at the sending client, and do not decrypt it at any point before it reaches the receiving clients."

Zoom clients include your computer running the Zoom app, a smartphone running the Zoom app and a Zoom Room, which are really only seen in large firms and enterprises. Essentially, your traffic is encrypted if all participants are using the app on a computer or smartphone. In that case, the user content is inaccessible to Zoom's servers or its employees.

The exposure for most people is when someone participates via a telephone call and not with the app or if the meeting is being recorded. Zoom cannot guarantee full encryption in those cases. There are other situations where full encryption may not be possible, but they are not commonly experienced by most lawyers. If you are really concerned about making sure that your Zoom meeting is as secure as it can be, require that all participants use the computer audio and do not allow telephone participation.

For those worried if Zoom can "tap" your session like a traditional communication channel, Zoom response is: "Zoom has never built a mechanism to decrypt live meetings for lawful intercept purposes, nor do we have means to insert our employees or others into meetings without being reflected in the participant list."

Zoom did not clarify the technical details for its encryption implementation. Without getting totally in the weeds, Zoom's encryption methods were not nearly as good as they could have been. Previously, Zoom used a single AES 128-bit key that was shared among all participants. Zoom also used AES in ECB mode, rather than a stronger industry standard.

To further improve security and respond to criticism about Zoom's encryption implementation, Zoom has released an update that implements AES-256 encryption instead of the weaker 128-bit version. Version 5.0 of the Zoom client was released on April 28, 2020 and is required for all Zoom participants as of May 30, 2020. All Zoom participants are now using AES 256-bit GCM encryption. Currently, the encryption keys are still stored and managed by Zoom while in GCM mode. The future implementation of end-to-end encryption for Zoom will put control of the encryption keys in the hands of the user.

Zoom rolled out phase 1 (Technical Preview) of E2EE with version 5.4.0 on October 26, 2020. End-to-end encryption is now available for all Zoom meetings (paid and free) with up to 200 participants. E2EE is not enabled by default, although you can make it the default for all meetings, which we do not recommend. You can always turn on E2EE on a per meeting basis and just leave the default as Enhanced encryption. If you do want to have an E2EE meeting, it must be defined at the time the meeting is scheduled by the host. In addition, enabling E2EE will require that all participants join from the Zoom desktop client, mobile app or Zoom Rooms. Users will not be able to join by telephone. You will also lose some features if you want to participate in an E2EE meeting. Enabling E2EE will disable allowing participants to join before host, cloud recording, streaming, live transcription, breakout rooms, polling and meeting reactions.

How will you know if the meeting is being encrypted end-to-end? Participants will have a green shield in the upper left corner of the meeting. You are in an E2EE meeting if there is a padlock in the middle of the green shield. Clicking on the shield will display the host's security code. The host can read the security code out loud and each participant can verify that they have the same code displayed.

Webex is currently the only other video conferencing system that has E2EE available and it is **not** enabled by default just like Zoom. By its very nature, utilizing E2EE will impact performance of your meeting as more processing and verification will be required for handling the data transmission. Even with the performance hit, we predict that Zoom will be able to scale better than Webex. Phase 2 of Zoom's E2EE rollout is currently scheduled sometime in 2021.

Ethical to Use Zoom?

Despite the media histrionics over Zoom's shortcomings, those shortcomings are shrinking day by day as security measures and privacy safeguards are implemented. We certainly believe that a lawyer's duty of competence (Model Rule 1.1) and the duty of confidentiality (Model Rule 1.6) are met if the lawyer has taken the time to understand the basic features of Zoom, including all security features.

Final Words

Zoom has become extremely popular. It is very easy to use even for those not technically inclined. Performance is good and there are lots of features to use. There are also features that can go awry. The jury is still out as to whether Zoom can be trusted or not. Are its intentions pure or did they just get caught? Certainly, we've seen some major improvements in the platform especially with the release of E2EE meetings.

Despite the concerns with Zoom's privacy and security, there is a practical side to using technology in your law practice. While it is desirable to control the encryption keys, the reality is that you can't always do that today. A lot of technology providers hold a master decryption key and could technically decrypt your data. Dropbox and Apple's iCloud are two that come immediately to mind. Another reality is that you can't really control what you cannot see at the other end of your communication. It doesn't matter if you are using Zoom, Webex, Teams, GoToMeeting or calling on your iPhone. You have no control over what the person on the other end is doing. They could have software installed that is recording your entire conversation and capturing video. A more old school method is to record with a separate device such as a voice recorder or even taking a video with your smartphone. Bottom line…nothing is 100% secure.

For now, we don't see any problem using Zoom for your video conferencing needs as long as the subject matter is not extremely sensitive. Be smart in how and when you use it. Spend a little time to become familiar with the capabilities of Zoom, especially if you are the one hosting the meetings.

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com.*