Zoom Training for Lawyers - and Using it Securely

Updated April 30, 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. 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 have been discovered and exposed by security researchers and journalists. Some of the publicity was just 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 is currently 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.

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.

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.

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 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 pretty 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 key 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 fairly 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. If enabled, the host can put the participant on hold, send them to the waiting room, etc.

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. 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 are scrambling to catch up. 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. Google just released an update to Meet that can only display up to 16 people simultaneously. Microsoft Teams is supposed to support nine people in a gallery view shortly. It seems like Zoom has won the gallery view battle.

Zoom has released an update that will be 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 a webinar. 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. There used to be a feature to let the host know if a participant is not paying attention, but Zoom has permanently removed that feature in a nod to privacy concerns.

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. 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 and co-host can freely move among the breakout rooms. However, that feature only works for the host at this time. The co-host must be assigned a room, but 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.

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. There will be an audio notification too if you have configured it. 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.

Once all the intended participants have joined, close the meeting. 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.

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) 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). 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.

Consider changing some of the default settings prior to scheduling the meeting. The first one is screen sharing. The default is to allow all participants to screen share. That means anyone can share their screen with inappropriate content. Yes, even bizarre sexual content. You definitely want to change the default to set screen sharing to host only.

Another 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. Zoom has changed the default settings in a recent release. 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 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.

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,” turn off the “Join before host” option. An alternate control mechanism is the Waiting Room feature. 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 “Join before host” option. You may have heard that there was a serious vulnerability with the waiting room feature. Independent research lab Citizen Lab did identify a problem and worked with Zoom to correct

the issue. Zoom has since corrected the security issue so it is safe to use the waiting room feature if you want.

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.

Consider turning on "Allow host to put attendee on hold" in the "In Meeting (Basic)" section. This will allow you kick people out of the meeting if necessary. Hopefully, you won't have to do that, but it's a good idea to have the option if needed.

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. 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 registration. 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. 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. You will only be prompted for the 2FA code when you sign into your Zoom account using a browser. Launching the Zoom app **does not** prompt for the 2FA code. Zoom protects

your account settings by enforcing 2FA from the browser. Logging in with your Zoom credentials when launching the app does not give you access to account settings so 2FA is less of a concern. The Zoom app is primarily used to impact the user interface while you participate in a meeting.

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 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.

Privacy

You need to understand that Zoom is constantly being criticized for its collection of data. It's rare that we come across an attorney that has actually read the Terms of Service, Acceptable Use or Privacy Policy. The Terms of Service for Zoom is thirteen pages, which may take you a little time to plow through. The interesting thing is that Zoom just updated its privacy policy on March 18, 2020. Coincidence or was it in response to the sudden spike in users flocking to Zoom?

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 with Zoom 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 has 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, China, Hong Kong (China), Japan, United States, Canada, Europe, India and Latin America. 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 and Canada to handle our Zoom traffic.

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. Recently, Zoom clarified their architecture and encryption schemes. The major criticism is the lack of end-to-end 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 are not nearly as good as they should be. A single AES-128 key is shared among all participants. Zoom also uses AES in ECB mode, rather than a stronger industry standard. Certainly, using AES-256 in a more secure industry standard mode would be preferred.

To further improve security and respond to criticism about Zoom's encryption implementation, Zoom has released an update that will implement AES-256 encryption. Version 5.0 of the Zoom client was released on April 28, 2020. You should manually update Zoom now to version 5 if it doesn't automatically update itself. Zoom will "flip the switch" to enable AES-256 encryption on May 30, 2020. If you have not upgraded to version 5, you will not be able to participate in any Zoom meetings after May 30th. Zoom has announced that a forced update will occur after May 30th if the update hasn't already occurred.

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 extremely 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. We would certainly like to see an improvement in the encryption and we need more time to assess Zoom's transparency promises.

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, 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. More old school 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.*