Getting Started with Zoom and Using it Securely

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 more popular video conferencing platforms is Zoom. There are others, but we see Zoom being used the most, especially among solo and small firm lawyers. While we can't cover all the options and settings for Zoom, we'll try to give our advice on the best way to use and secure Zoom for your firm.

Basics

The first question 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 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 don't 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.

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. Objects behind you may be distracting too. Think about what the person on the other end is seeing. Be cognizant of those around you too. Family members may be able to hear you discussing confidential information even if you are wearing a headset.

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 where 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 is even an option to let you know if a participant is not paying attention.

Another helpful feature for mediators is the Breakout Room feature. You create the rooms and then assign participants to a specific room. 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.

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 off, 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.

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. Once all the intended participants have joined, close the meeting. You do this by selecting “Manage Participants” and then click “More” at the bottom of the panel. 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 without those barriers.

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.

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? In the “Schedule Meeting” section of “Settings,” turn off the “Join before host” option.

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.

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 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 meeting ID.

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 by selecting "Security" in the "Admin" section, under "Advanced." Turn on the "Sign in with Two-Factor Authentication" option.

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.

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."

Another Zoom criticism is the ability to determine if attendees are paying attention. There is an "Attention tracking" setting that monitors when a participant has clicked focus away from the Zoom window for more than 30 seconds. Some users call it the "boss is watching" feature to see if you are doing other things while your boss is pontificating.

Final Words

Zoom has become extremely popular. It is extremely easy to use even for those less technically inclined. Performance is good and there are lots of features to use. There are also features that can go awry. 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.