A videoconference deposition primer

by Cory H. Morris and Victor John Yannacone, Jr.

C. MORRIS

V. YANNACONE, JR.

Introduction

The COVID-19 pandemic should be a wake-up call to attorneys and law firms using systems dating back to the era of manual typewriters, carbon paper, and secretaries with steno pads taking shorthand notes while lawyers dictated, or lawyers filling pages of yellow legal pads with drafts to go to the typing pool. The social distancing required to limit the spread of the COVID-19 virus is forcing us to eliminate nonessential face-to-face contacts and challenging us to redefine essential face-to-face contacts.

The pandemic has "virtualized" all sorts of pretrial tasks. By the time we return to our offices, we all should have been looking long and hard at what aspects of litigation in the federal and state courts actually need in-person appearances.

Remember, attorneys have a nondelegable obligation to remain technically competent in times of crisis and change.

According to the American Bar Association Model Rules of Professional Conduct (RPC):

> Rule 1.1 Competence. A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

In August 2012, Comment 8 was added to the Rule:

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology …

As ethics opinions throughout the country make clear, that mandate includes "at a minimum, a basic understanding of, and facility with, issues related to e-discovery, including the discovery of electronically stored information (ESI)," adding this ominous warning to the unprepared attorney: "Lack of competence in e-discovery issues also may lead to an ethical violation of an attorney's duty of confidentiality."[1]

The California State Bar established three options for attorneys "lacking the required competence for e-discovery issues": (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; and (3) decline the client representation.

The RPC will no doubt require attorneys to become familiar with platforms like Zoom, Skype for Business, and Microsoft Teams. Court reporting services are quickly seizing the opportunity to provide professional videoconference deposition services in addition to conventional stenography.

The vast improvements in video recording, internet communication, and cloud-based systems should allow trial attorneys to reconsider the basic elements of litigation in federal and state courts. Many courts have already begun utilizing advances in telecommunications technology by excusing personal appearances for case management conferences and motion hearings and by conducting pretrial conferences by teleconference. Attorneys should be quick to take advantage of modern technologies to make the nature of litigation more cost effective.

Deposition by videoconferencing is not the same as a videotape deposition

At the dawn of the computer age, the admonition "read the manual" was known as the First Commandment of Technology. It bears repeating that you should read the manual.[2]

The Federal Rules of Civil Procedure allow for depositions to be conducted by remote videoconference or telephonically. While there are slight variations among jurisdictions in the procedure and circumstances under which depositions can be conducted remotely, almost every jurisdiction allows it as an acceptable and permissible practice.

Notice of the deposition by videoconference

In both state and federal actions, parties should provide notice of a videoconference deposition, notice of the videoconferencing software that is to be used, and that the video deposition conference will be recorded. To avoid misunderstandings, the notice should also state that a simultaneous stenographic transcription of the testimony will be made.

If the notice was originally served without the appropriate language, an amended or supplemental notice should be served as soon as possible and within a reasonable time prior to the deposition. If the supplemental notice window has passed, either obtain a stipulation from opposing counsel or an order from the court.

Court reporter compensation is important. At the time a video deposition is scheduled, the parties should agree that the entire cost of the deposition as charged by the court reporter, including the cost of video recording and processing, should be recoverable as "costs by the prevailing party" if not borne by the parties individually. If the parties cannot agree, an order of the court resolving the issue should be obtained.

Parties to a video deposition should insist that the court reporter as well as any videographer other than the court reporter disclose on the record at the start of the video deposition whether any contract exists between the court reporting service, the court reporter, and/or any videographer and any of the parties or counsel in the litigation.

Should the parties disagree regarding the mechanics or conditions of a video deposition, any objections must

Videoconference
from preceding page

be raised at the time of the deposition or else such objections are waived.[3]

Hardware concerns such as lighting, a strong and stable internet connection preferably hardwired rather than Wi-Fi, and a proper directional microphone for the witness should be included in the preliminary arrangements for any videoconference deposition.

Location and jurisdiction matters

Notice and the administration of the oath are important.

Rule 30 of the Federal Rules of Civil Procedure requires "reasonable written notice to every other party, stat[ing] the time and place of the deposition and, if known, the Witness's name and address." The court reporter who is administering the oath should obtain photo identification consistent with the jurisdiction. When possible, parties should stipulate, among other things, admissibility of the recording of the videoconference deposition as well as the stenographic transcript.

Both Florida Rule 1.310[4] and the Federal Rules of Civil Procedure allow for video recording; however, in the case of recording a videoconference deposition, a stipulation or a court order is appropriate. Rule 30(b)(3)(B) allows "[w]ith prior notice to the Witness and other parties, any party may designate another method for recording the testimony in addition to that specified in the original notice."[5]

"[T]he Florida Rules of Civil Procedure provide means by which parties or witnesses may present testimony when their physical presence is not possible at a civil trial or hearing. For example, Rule 1.310 provides that testimony of any party to a civil suit may be taken by deposition, which may be recorded stenographically, videotaped, or taken by telephone."[6]

Best practices should include not only meeting the statutory requirements but notice that the deposition will be taken via electronic means, and the device(s) and internet service requirements necessary for the witness to participate. Should it be necessary, one can arrange to have the witness testify at a location where the court reporting service will make all the necessary video, audio, and social distancing arrangements.

The videoconference deposition "road test"

Plan logistical details for a deposition by videoconference far in advance and test everything possible. Make sure that all the necessary parties to the deposition have a reliable and high-speed internet connection, a webcam, and the software necessary to participate on the videoconferencing software platform.

Test the video feed before the deposition to ensure that any lags or delay in the audio or video streams can be addressed before the deposition begins. Multiple devices connected to one internet connection will usually use more bandwidth and often slow the video feed.

Have the court reporting service test the software platform in advance as well as the communications with the parties participating in the deposition.

Test the method by which exhibits will be introduced and that they can be shared with the witness and all counsel. Make sure there is an agreed upon plan for showing the exhibit to the witness, allowing the witness and his or her counsel to examine and read the exhibit, and allowing the court reporter to make the exhibit part of the record.

Some commercial services have specialized electronic systems that allow you to upload exhibits in advance and then "publish" such exhibits in the same window used for the videoconference deposition.

Be wary and beware of backgrounds

Some commercial technologies offer virtual backgrounds, which have the added benefit of avoiding unintended, unfortunate visual interruptions such as a child or a pet wandering into view. If you choose to use a virtual background, be sure to avoid these pitfalls: wearing clothing that blends into the background; choosing a background that could be considered unprofessional; or using a background that is distracting to others on the videoconference.

Internet issues

Good internet bandwidth is essential. Every participant should be using a dedicated and stable high-speed internet connection during the deposition. If your internet connection is being shared with Ring doorbells, Amazon Firesticks, streaming Netflix, and VOIP while the children are participating in online classes, you will likely have poor internet bandwidth.

Before the deposition begins, test your ability to obtain a full picture (hands on the table, shoulders and head in the image) video of the witness and whether you have a solid internet connection with all the required programs running. Check your internet speed on sites such as SpeedTest.net.

The videoconferencing service provider

The most common service providers that attorneys will see are the courts, government agencies, and court reporting services that will be taking testimony under oath. They will often collect information from all participants such as names, roles, organizations, email addresses, usernames and passwords, as well as information about devices they use. Make sure you know how this information will be used by a service provider.

Look for these features and benefits from your video service provider and verify with your court reporting service that the system meets these criteria:

- End-to-end secure encryption with meeting-specific key logins
- Secure file sharing that allows for viewing during live videoconferencing
- Control of chat features during the videoconferencing
- Compatibility with all browsers, including Chrome, Edge, Firefox, and Safari
- Full HD audio and video
- Full audio and video recording of the videoconference deposition with full indexing

Prepare for technology breakdowns

During videoconference depositions, the most likely failure is an

Videoconference
from preceding page

internet connection problem. Have your court reporting service test the internet connection.

A new role for clients in depositions by videoconference

It is a good practice to invite your client to participate in the videoconference deposition as a silent observer. The use of remote videoconference depositions allows clients to attend depositions without being seen or heard.

Clients who listen and take notes on the testimony can propose follow-up questions that help with technical issues or place certain testimony into the appropriate context and often provide valuable insight. Non-lawyer clients can appreciate and understand the testimony as a juror would. Breaks during the deposition allow an attorney and his or her client to interact and exchange notes on any follow-up inquiries or additional lines of questioning.

Conducting the deposition by videoconference

Depositions should start promptly. A confirmation and oath will be taken of the deponent by the court reporter who will have already recorded the deponent's picture identification.

All counsel must identify themselves to the satisfaction of the court reporter, and all the parties should note their appearance on the record. The court reporter is the "host" for the videoconference and should identify everyone else present on the videoconference and confirm that the videoconference is password protected.

The actual physical location of each party should be identified and each participant asked whether any other individuals are in a position to observe or listen to the deposition at their location. If so, all such observers and eavesdroppers should be identified on the record.

The witness actively participating in the deposition should be "pinned." The "pin" video feature on Zoom allows you to disable active speaker view and only view a specific speaker. It will also only record the pinned video if you are recording locally (to your computer).

Specific witness instructions for videoconference depositions

Because of differences among internet service providers (ISPs) and the nature of the connection each participant in the videoconference deposition makes to his or her ISP, there may be time delays in the questions and answers. The first time this phenomenon is observed by any party to the deposition, a note should be made in the record. This becomes important if the actual videoconference recording rather than just the transcript is used at trial.

Deposition instructions that direct the witness not to have any substantive discussions with his or her counsel during breaks from the deposition also become more important given the remote nature of the proceedings, and the witness should be reminded of these instructions before any break is taken.

Objection for one; Objection for all

Remote depositions present difficulties in raising objections in a timely manner before the witness answers, leading to attorneys talking over one another on the video feed in order to preserve their objections or leading an attorney to believe an objection was raised when it was not recorded by the stenographer.

The simplest solution to this issue during a remote videoconference deposition is an agreement or stipulation between counsel that an objection raised by one party is deemed made by all other parties.

Carefully consider off-site collaboration

Remote depositions by teleconference permit participants other than the witness to utilize private chat or text message features on devices not connected to the videoconference such as cell phones, tablets, and laptops that enable participants to discuss important issues and responses raised during the deposition without the need to take a break for off-the-record conversations. The potential for coaching the witness is obvious.

It is important that remote depositions allow for a clear and uninterrupted view of the deponent. Make sure you can see the hands of the witness at all times and that you know what the objects are in the line of sight for the witness throughout the deposition. There should be nothing behind the video camera other than the court reporter, or if the court reporter is not in the same room as the witness, make sure the background seen by the camera is a blank wall or a bookcase. Ask the witness to use the computer video camera connected to the videoconference and scan the entire room so that all entrances and exits are identifiable as seen by the witness.

Breaks

Depositions by videoconference will provide all the parties access to the full audio and video of a witness in his or her "natural" environment, typically his or her home or office. An attorney will probably not be in the same room as the witness. The time of every break and the reason for the break should be noted on the record. The video and audio of the videoconference should be muted during breaks.

Exhibits

Commercially available videoconferencing software platforms permit uploading exhibits and documents in real time during the deposition or in advance at a "Meet & Confer" teleconference[7] and refer to them in real time during the videoconference deposition. This becomes more important as the number of documents in a case increases.

Certain platforms allow the attorney and the witness to incorporate electronic markings on a document in real time, such as highlighting or call-out boxes, to emphasize critical portions of the document such as relevant contract language or accident scene photographs. These markings can then be saved as part of the exhibit for later use as part of any dispositive motion or at trial.

All the parties to a deposition by videoconference should demand that any documents intended to be used during the deposition be distributed to all parties a sufficient time in advance of the deposition (typically five days).

Screen sharing allows you to access open documents and programs on

Videoconference
from preceding page

your computer. With screen sharing, a lawyer can freeze the frame and get the witness to testify about the image or audio, all while creating a permanent video record of the process as part of the deposition.

More advanced settings allow for reference to exhibits from a variety of applications and sources including second screens or tablets the witness can be asked to mark or annotate in real time, which may then become new exhibits.

Courtesy and civility rules for depositions by videoconference

- Give the court reporter time to get all the appearances before starting the deposition.
- If you are not questioning, mute your microphone.
- Place your computer or microphone as close to you as possible.
- Don't rustle papers near the microphone.
- Speak slowly, particularly when reading from documents.
- Give the court reporter time at the end of the deposition to check any spellings with the witness before everyone jumps off the call.
- Be patient!

Cybersecurity for depositions by videoconference

Web conferencing solutions were originally called online collaboration tools and provide audio/videoconferencing, real-time chat, desktop sharing, and file transfer capabilities.

As the convenience and efficiency of depositions by videoconference becomes more apparent to attorneys and the federal and state courts, many attorneys are using Zoom because of its reliability and ease of use. Zoom, however, is not inherently secure. It requires some positive action on the part of its users.

First, make sure everyone in a Zoom meeting connects using "computer audio" instead of calling in on a mobile phone. Then make sure that the host for the conference, meeting, or deposition starts with the "Require Encryption for 3rd Party Endpoints" setting *enabled* and a padlock has appeared that says "Zoom is using an end to end encrypted connection" when you mouse over it. Without that padlock, do not expect your conference to be secure or even private.

Even with the padlock, Zoom has the technical ability to spy on private video meetings and could be compelled to hand over recordings of meetings to governments or law enforcement. While companies like Google, Facebook, and Microsoft publish transparency reports that describe exactly how many government requests for user data they receive from which countries and how many of those they comply with, Zoom does not.

Major security threats

- **Zoom bombing** where someone disrupts your meeting with disturbing or pornographic images and videos
- **Snooping** where an outside party listens in on your online conference and can compromise sensitive information
- **Hacking** particularly where the web conferencing platform stores the information of participants and users for some time, as well as files you've uploaded

The Health Insurance Portability and Accountability Act (HIPAA) makes it a crime to not appropriately secure patient information. The Gramm-Leach-Bliley Act (GLBA) financial privacy rule requires businesses to be transparent about how they protect consumers' information, including data stored within web conferencing platforms.

Violations can lead to severe fines and lack of confidence among clients.

FedRAMP Compliance

The National Institute of Standards and Technology (NIST), which is the American equivalent of the ISO (International Organization of Standards), implemented the Federal Information Security Management Act (FISMA) with the Federal Risk and Authorization Management Program (FedRAMP). If the web conferencing platform you use is FedRAMP certified, you can feel confident you're well protected.

International organizations look for a platform to be ISO 27001 certified. If your web conferencing platform is FedRAMP compliant, it will hold the "Agency FedRAMP Authorization" title.

Hosting a videoconference deposition

Unless there is some court-approved justification, the host of any videoconference deposition should be the court reporting service. Depending on the videoconferencing deposition software platform, the host is the administrator and manager of the videoconference. The host has unique privileges and responsibilities including but not limited to:

- **Necessary access restrictions** include passwords for hosts before they open a virtual room; codes for participants before they join; limits on the hours a virtual room can be accessed; monitoring remote users; and only handling and exchanging encrypted information.
- **Session locks** should be set by a host restricting access to participants who show up late and avoiding unwanted visitors.
- **Credential termination**, which prevents readmittance without new credentials/passwords, should occur whenever a member electronically leaves the hosted space.
- **Role-based access controls** (RBAC) define the levels of interaction users can have in a platform and are particularly useful with large conferences. The level of control descends from the host, who has most control, through presenters with less control to participants with least control. The host owns the online room and can set access requirements. Hosts manage the content uploaded and the interactions of the room.
- **Dynamic privilege management** allows a user to retain his or her virtual identity when access privileges are temporarily upgraded or limited.
- **Blacklisting** permits an account administrator to limit which features appear in users' virtual rooms.
- **Disabling functionality** is the

Videoconference
from preceding page

ability to block screen sharing for certain applications or programs.

- **Whitelisting** is often a better option than blacklisting because you limit screen sharing to just what you need.

Although an attorney should not be the host for a videoconference deposition, the attorney noticing the deposition must consider how invitations, website links, and access credentials will be distributed to participants.

- Do not share website links or access credentials on publicly accessible websites or social media.
- Limit credentials to a single event.
- Do not reuse online access credentials.
- Only allow invited participants to join the deposition.
- Once all participants are present,lock the videoconference so no one else can join.
- Make sure you completely identify each individual participant on the record.
- Only share what is required and as little as possible. If screen sharing is not required, either disable the functionality or limit its use to only the meeting host.

Encryption

The standard for securing the recording of a videoconference deposition is AES 256-bit encryption. A good web conferencing provider will encrypt the recording while in storage and transmission, while the best providers also keep logs of interactions with encrypted materials. If your recordings are encrypted, anyone who interacts with them will be identified.

The service provider should be encrypting data both while it is at rest and stored by the service provider and while it is being transferred between different devices. Make sure your web conferencing system uses strong encryption, such as Transport Layer Security (TLS), to protect data while it is in transit. TLS versions 1.2 and 1.3 inherently offer more protection for data transmitted across untrusted networks such as the internet.

Zoom alternatives

Group FaceTime for Apple products supports up to 30 callers and provides end-to-end encryption; however, it is not cross-platform.

Microsoft Skype handles up to 50 people in a videoconference or 150 people in a group text chat. Skype also supports group video chat and is available on most platforms. Skype offers document and screen sharing but, *beware*, Skype conversations are not end-to-end encrypted.

Webex allows one to host up to 200 participants, up to 10 GB of encrypted cloud storage, branding and customizations, domain claim, syncing with Microsoft Exchange and Active Directory sync, and TLS (Transport Layer Security) 1.2 support.

Microsoft Teams supports 2FA (two-factor authentication) security, data encryption, and meets dozens of national, regional, and industry-specific security/privacy compliance regulations. It also integrates extremely well with Microsoft's other productivity products, including Office 365.

There are more complex and expensive options such as Cisco Webex Meetings, TeamViewer, and GoToMeeting. Webex Meetings offers end-to-end encryption as an option.

Another highly secure solution, *Signal*, supports video collaboration and offers end-to-end encryption. It is a full-featured collaboration solution, works on most platforms, and lets you share all messages, photos, videos, files and chat using video. *Signal* is free.

A model online deposition by videoconference order

The basic terms of an order for a videoconference deposition should include, among other case-specific terms, the following general instructions:

1. All applicable jurisdictions' Rules of Civil Procedure and Rules of Professional Responsibility governing the practice of law remain in place and in full force and effect and shall be followed at all times. This includes, but is not limited to, the prohibition on speaking objections and prohibited contact with a witness during the course of a deposition.
2. The court reporter for a deposition conducted via videoconference, in accordance with Supreme Court of Florida's AOSC20-16 issued on March 18, 2020, may administer the oath or affirmation to the deponent remotely.
3. The witness may elect to physically exclude any person from any room where the witness is physically present during the taking of the deposition. Any counsel of record or party so excluded by the witness may participate in the deposition by means of videoconference.
4. No other attendees other than the parties to the subject lawsuit, their representative counsel, and counsel for the witness shall be allowed to participate in the videoconference deposition without prior consent of all counsel. This includes appearing individually within the videoconference platform and/or being present within the room where the attendee is viewing the videoconference deposition.
5. The court reporter's transcript shall serve as the official record of the witness's testimony. Should circumstances arise that render the court reporter's transcript unavailable, then a new transcript can be created from the video recording of the deposition.
6. Any deposition taken by means of videoconference shall be conducted using a videoconferencing platform generally acceptable within the industry and equipped with the ability to video record the deposition. The court reporter shall serve as the host of the videoconference as provided by the videoconferencing platform.
7. As the host of the videoconference, the court reporter shall video record the witness using the recording function of the videoconferencing platform. Alternatively, if a videographer is provided by the court reporting service, such videographer may

Videoconference
from preceding page

control the recording function of the platform. The court reporter or videographer, as the case may be, shall also announce each time he or she has activated and deactivated the record function on the videoconferencing platform, and such statements shall be made a part of the transcribed record. In addition, any party may at its discretion arrange for an independent videographer to video record the deposition by means other than the video-recording function of the platform. The party hiring any such independent videographer is responsible for the costs of doing so and must make copies of the video recording available to all counsel at their expense.

8. The video recording of the deposition created by use of the recording function of the videoconferencing platform shall be deemed the equivalent of a video recording made by a videographer, and shall be available for use in trial as though prepared by a videographer.

9. No participant in the deposition may utilize the chat function or similar private communication function of the videoconference platform, except to facilitate the sharing of documents during the deposition. In no event shall the chat function or equivalent means of communication be used for any counsel to communicate directly with the witness.

10. At no time during the deposition shall any counsel text, message, email, or transmit any messages to the witness(es) in order to help the witness(es) respond to any and all questions.

11. Before the witness is sworn, all cellphones shall be placed in the silent mode. All parties and counsel participating in the videoconference will disable notifications and other functions on their devices that might disrupt the audio and/or video stream during the deposition.

12. The witness and all counsel or parties appearing on the record shall state their appearances clearly for the record, and they shall not disable their cameras during the deposition unless there is a break or unless they are necessarily appearing by telephone.

13. All documents or other exhibits, except those to be used for impeachment, shall be shared with all counsel no later than three (3) days prior to the deposition, and said documents shall be Bates-stamped, marked as exhibits, or both. Electronically stored information (ESI) not suited for Bates-stamping or marking as exhibits may be identified by prepending a number or other identifier to the name of each file. Such changes to a file name should be non-destructive and reversible using freely available tools such as Bulk Rename Utility for windows (https://www.bulkrenameutility.co.uk/) or the "Rename Finder Items" function in the Mac operating system.

14. As to non-party witnesses served with a subpoena duces tecum, counsel or their designee for all parties are permitted to confer with the witness for the exclusive purpose of securing any and all documents or other relevant evidence responsive to the subpoena duces tecum. This shall take place no later than five (5) days prior to the scheduled deposition. No later than one (1) business day prior to the deposition, all documents shall be provided to the court reporting service. Those documents or other exhibits used for impeachment must be shared with all participants when introduced on the record via the share screen or similar feature on the videoconferencing platform and attached as an exhibit to the deposition.

15. If the video connection is lost and cannot be restored within a reasonable length of time, the deposition may proceed and the witness may testify telephonically.

A final comment

Whether it is your very first deposition or your very first electronic deposition, the technology and practice may be novel but it is not difficult. For better or worse, technology will be utilized at every available opportunity to maintain social distance. Like riding a bike, however, once you have it down, it will become second nature.

Endnotes

1 Formal Opinion No. 2015-193, State Bar of California, http://ethics.calbar.ca.gov/Ethics/Opinions.aspx

2 For Zoom, access the tutorial at https://support.zoom.us/hc/en-us/articles/206618765-Zoom-Video-Tutorials

3 Fed. R. Civ. P. 32(d)(3)(B).

4 *See*, e.g., *Gosby v. Third Judicial Circuit*, 586 So. 2d 1056 (Fla. 1991).

5 Fed. R. Civ. P. 30(b)(3)(B).

6 *Gosby v. Third Judicial Circuit*, 586 So. 2d 1056, 1058 (Fla. 1991).

7 Fed. R. Civ. P. 16, 26.