Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# Anticipate Gov't Subpoenas Of Your Zoom Recordings

By **Dan Zelenko, Nimi Aviad, John Davis, Rukiya Mohamed and Bridget Carr**
(April 23, 2020, 5:37 PM EDT)

Dan Zelenko

Nimi Aviad

John Davis

The novel coronavirus pandemic is forcing us to work, learn and socialize remotely. Videoconferencing solutions like the one provided by Zoom Video Communications Inc. have proved helpful in keeping governments running, companies and organizations working, and friends and families connected.

Businesses across the country are turning to these technologies on an unprecedented scale. They also are making and keeping recordings of these calls, which the government and litigants may view as discoverable.

This is not a theoretical issue; in recent days, government investigators have asked some of our clients about videoconference recording practices and the availability of responsive recordings in the context of ongoing investigations. The following explains the issue and offers best practice recommendations.

**Government Requests for Zoom Recordings**

Zoom is a videoconferencing application that allows many users to be in the same virtual room at once. Although the application (or the concept) is not a new one, Zoom has emerged as a go-to tool for maintaining connections during the COVID-19 pandemic.

Zoom's popularity in the corporate setting is particularly noteworthy given that its designers apparently did not view it as an enterprise communications platform. Zoom's consumer-oriented design and user-initiated interface mean that centralized information technology oversight is not fully enabled in the system, as with other enterprise-minded solutions.

Further, its informality engenders the sort of instant takes and informal behavior that can lead to misunderstandings when recorded. This raises a number of concerns from a legal and compliance perspective.

In government investigations, video recordings have often taken a back seat to other (usually text-based) forms of evidence. The reason is that in-person meetings, which are rarely recorded, were far more common than legacy videoconferences, and the latter were typically conducted through enterprise teleconferencing systems with clear rules and controls around recording.

Rukiya Mohamed

In our current, COVID-19 reality however, videoconferences are used en masse; they have replaced even impromptu in-person meetings and often are being conducted on systems that have not gone through normal corporate onboarding processes.

Government investigators have noticed and are not passing on the opportunity to capture this new source of information. While video recordings have long been a standard part of government requests, the speed at which the government is adapting to this new reality and seizing on the opportunity to collect Zoom recordings may catch certain companies — new to Zoom themselves — off guard.

Bridget Carr

The government's common existing subpoena or investigative demand language is typically quite broad and would likely already encompass Zoom's videoconference recordings.

A common U.S. Securities and Exchange Commission subpoena for documents, for example, defines a "document" to encompass information recorded by any photographic process, including video recordings. This means that any video recording made by company employees that is responsive to the SEC's substantive subpoena request must be preserved and turned over.

Most U.S. Department of Justice grand jury subpoenas, too, define "document" to include electronically stored information of any kind in the company's possession, custody or control. This arguably includes recordings of Zoom videoconferences residing on company servers.

Companies unaware that employees are creating this uncontrolled form of evidence may find themselves playing catch-up. Conversations that previously had gone unrecorded, and for which no business reason exists to maintain, may now be subject to remediation, preservation and production.

**The Cost of Producing Video Recordings**

Aside from creating additional evidence for government investigators, responsible compliance with the government's new requests in this new normal may be costly. Unlike other documents, video recordings are difficult to search. They generally must be reviewed from beginning to end, often multiple times to catch cross talk and speech irregularities.

While some technology can be helpful in this process, solutions are perhaps ten years behind the development of text-based analytic tools in their functionality and effectiveness and present further new costs. To avoid the complications and expense associated with these production companies should ensure that they have appropriate controls in place to manage the creation of Zoom and other video recordings. Where recordings have already been made, controls should help companies comply, effectively and efficiently, with government requests.

**Best Practices**

Employers must consider both current obligations and future plans in order to create an effective strategy for the use and preservation of videoconference recordings.

As for current obligations, the entity must figure out whether a potential preservation triggering event, such as a government subpoena or other form of demand, has taken place. An entity that reasonably anticipates or has received a demand for information from a law enforcement or investigatory body has a duty to preserve existing, potentially responsive recordings in its possession, custody or control.

As noted, videoconference recordings would arguably fall under the definition of document in most government-issued requests. While burden and proportionality arguments will often be raised in civil matters, such arguments may find little traction in governmental inquiries, and companies should think hard before unilaterally taking action not to preserve video files based on those rationales.

If an entity does not have an affirmative duty to preserve its Zoom or other video recordings, this is the right time to think critically about future plans: whether and how to permit use of Zoom's recording capabilities. To establish best practices:

- Onboard Zoom and other videoconference tools through your normal IT process.

- Consider which meetings should be recorded and which should not, and determine how long recorded meetings should be kept; then establish clear rules for users to follow.

- Research existing laws and policies that govern audiovisual recordings of company events and meetings.

- Implement and train users on a new or updated policy that clearly establishes when, where, how and for how long Zoom and other videoconference recordings should be captured and stored.

***What Should Be Recorded?***

When considering what should be recorded, many companies have determined to block and prohibit the recording of any videoconference, unless required by statute or regulation or authorized by an established exception to the above policy (for example, when there is a clear business purpose). Approved methods of note-taking should instead be encouraged, despite Zoom's ability to provide a nearly automatic and low-cost way to create a perfect record.

Employers must also consider right-to-record and privacy issues implicated by the use of video recordings. Regulations as to participant personal information and notice and consent of recordings vary by jurisdiction and can be impacted by company-specific employment policies. These issues are important and require a company-specific detailed analysis.

***Storage Options***

If recording Zoom videoconferences is nevertheless desired (or required), consider storing recordings on company-controlled storage with adequate encryption capabilities rather than on Zoom's cloud-based storage. Company storage of Zoom recordings should be implemented through a customized IT structure designed to collect, store and preserve the recordings in an adequately protected, central and organized fashion.

The system should be set up with e-discovery and information management considerations built in, so that files may be identified, extracted, and deleted without ruinous effort. Finally, the policy should call out designated managers responsible for maintaining and auditing the stored information to ensure that established use policies are followed.

Company-controlled storage does not only provide greater control over review and distribution of these records. It also prevents government investigators from gaining access to business-sensitive information without an entity's knowledge or consent through the use of a third-party subpoena served on Zoom or another cloud-based platform holding the data.

***Communicate the Policy***

After establishing best practices, disseminate the information widely among the workforce. Zoom's easy-to-use platform demands clear, transparent and user-friendly guidelines informing employees how to use Zoom's recording features. Consider using Zoom's built-in administration tools to control, on the back end, a host's ability to record meetings, per the established policy.

**Conclusion**

Even when compliance resources are spread thin, the recent increase in the use of Zoom and other videoconference platforms calls for a policy that permits employees to continue and use this now-critical technology, while protecting the company's interests. The government's apparent interest in Zoom recordings for its investigations should serve as an incentive to take on this issue now.

---

*Dan Zelenko and Nimi Aviad are partners, John Davis is senior counsel, and Rukiya Mohamed and Bridget Carr are associates at Crowell & Moring LLP.*