

Lawyer Insights

Litigation Risks of Videoconferencing Tools

By Paul D. Ackerman and Christopher M. Pardo
Published in Risk Management | July/August 2020



Seemingly overnight, the business world experienced the widespread adoption of videoconferencing technology such as Zoom, Skype, Webex, Microsoft Teams and Google Meetings to keep employees connected during the COVID-19 pandemic. As with email, text messaging and other electronic communication tools, a byproduct of the use of videoconferencing is the tremendous amount of data now being generated and stored. If not managed properly, this data could become a significant litigation risk.

While the specific features of each videoconferencing system vary, these platforms generally allow users to configure robust storage options, including usage reports, records of all participants, automatically generated transcripts, and audio and video recordings. Many offer cloud-based storage, and some platforms also allow local storage, where a copy of the data from a videoconference can be stored on individual machines apart from the central cloud-based repository. Essentially, terabytes of additional data may be stored and distributed across your enterprise, creating challenges for data collection.

In the world of litigation, the data created by electronic communication tools is known as electronically stored information (ESI). In significant legal cases, courts generally require that relevant ESI be provided to the opposing party during discovery. Large amounts of ESI can lead to a burdensome and expensive discovery process for the producing party. On top of that, ESI can be a potential gold mine for the requesting party, as more informal communications like email and text messages frequently provide unfiltered thoughts and comments, often without appropriate context, which can be damaging in the context of a lawsuit.

For example, consider a product liability lawsuit alleging that a newly developed product is defective. The development process involved a six-person team working for over a year to bring the product to market. During development, the team held weekly team videoconference meetings to discuss all facets of the project, including every problem with the product, whether real, perceived or hypothetical. The team members also had regular videoconferences with others outside the core team, including vendors, contractors, consultants, other company employees and the management team. From this relatively modest development project, potentially hundreds of hours of video, audio and related data on meeting transcripts, attendance and the like were generated and stored by the videoconferencing system.

All of this ESI may be subject to discovery in the product liability lawsuit. If so, this data will need to be collected and reviewed by attorneys and potentially produced for the other side. Moreover, every word and gesture from every meeting will be available for the other side to review and be shown to a jury. Even

Litigation Risks of Videoconferencing Tools

By Paul D. Ackerman and Christopher M. Pardo
Risk Management | August 3, 2020

good-faith efforts by the team to identify and solve potential problems along the way may be viewed as knowledge of a problem. This could ultimately prove disastrous.

Properly managing this new wave of ESI data is critical and should be done before you face any litigation. This requires two main actions: 1) developing and implementing sound data retention policies that address the vast amounts of information generated by your videoconferencing platform, and 2) providing employee training to mitigate the risks inherent in this growing body of potentially discoverable information.

A data retention policy is a formal policy that addresses how your organization will maintain various business records and when those records should be deleted. Take care to create a policy that fits your business needs without requiring that you perpetually store every bit of generated ESI. This requires understanding the needs of your business and the features of the videoconferencing tool it is using. For example, every company should consider the following questions:

- For the specific videoconferencing platform(s) being used by your enterprise, what data is automatically stored, and what data can be optionally stored?
- Who has the ability to control storage settings and options? Are they set by the system administrator or each user?
- Where is the data stored?
- What administrative tools are available through the system to automatically manage data retention? Who can control these settings?
- What is the business value of maintaining each type of record? How long do these records need to be maintained? Is there a business need to record most videoconferences? If so, how long does this data need to be stored?

With this information in hand, the company can work with legal counsel to update videoconferencing use and data retention policies to properly limit the ESI to only what is essential to the business.

In addition to data retention, effective risk management should include updating employee policies and related training on the proper business use of videoconferencing. It has become commonplace in litigation over the past decade for emails and text messages obtained through discovery to reveal startling statements that dramatically influence the outcome of a dispute. The ease of use of these tools fosters a level of informality in communications that can seriously jeopardize a case. With videoconferencing, not

Litigation Risks of Videoconferencing Tools

By Paul D. Ackerman and Christopher M. Pardo
Risk Management | August 3, 2020

only will cavalier statements during meetings be made available for discovery, but facial expressions, hand gestures and overall body language may also be recorded and played for a jury.

So not only is this vast collection of data expensive to maintain, gather, review and produce during litigation, a moment of poor judgment by a single employee captured during a videoconference—even when that employee's thoughts may not be shared by others in the room or the company's management—may prove damaging.

Companies should update employee manuals and provide additional training to highlight that videoconferencing may be an important business tool, but its convenience and ease of use should not invite foregoing good judgment. In fact, it is important that employees exercise an even greater level of discretion when using videoconferencing. Employees should be trained to assume that each videoconference is being recorded and, if for any reason they would be uncomfortable having their statements, facial expressions or gestures played back to a jury, they should not be engaging in such conduct during a videoconference. Videoconferencing platforms have been a tremendous asset during the pandemic and will likely continue to be an important tool even after the current crisis is under control. As with other communication tools, however, proper management is essential to help your company reduce future litigation risks.

Paul D. Ackerman is a partner in the firm's Intellectual Property group in the firm's New York office. Paul's practice involves all aspects of intellectual property and technology law with an emphasis on patent litigation and trial. He can be reached at +1 (212) 850-2858 or paulackerman@HuntonAK.com.

Christopher M. Pardo is a partner in the firm's Labor & Employment group in the firm's Boston office. Chris focuses his practice on the defense of complex employment cases in federal and state courts, arbitration, and before administrative agencies. He can be reached at +1 (617) 648-2759 or cpardo@HuntonAK.com.

Reprinted with permission from *Risk Management Magazine*. Copyright 2020 RIMS, Inc. All rights reserved.