How to Protect Your Business While Working Remotely

Gina Vitiello— April 10, 2020

These days, most offices across the globe remain empty while employers have little to no choice but to operate with a remote workforce. Online meetings are now being used to discuss important decisions that once took place in conference rooms. While businesses continue to operate in this fashion, employers must consider whether and when it may be appropriate to use these online meeting platforms and understand the risks involved relating to privacy.

Although laws may offer some privacy protection regarding live conversations via a telephone line, there is a lot of gray area still when it comes to stored communications conducted via online meetings. Additionally, many companies do not have policies or guidelines for using, recording or storing online meetings–especially those companies that are using online meetings as a communications tool for the first time during this crisis. The technology exists to record and disseminate such meetings, so the main questions then becomes: What must meeting organizers do to guarantee the content of an online meeting will be kept confidential?

One thing meeting organizers can do is to limit the use of online meetings for highly confidential or sensitive matters unless there is a need to share electronically stored information. While online meetings more closely resemble face-to-face meetings because of the ability to see the participants, the images and voices (and any on-screen presentation materials) become “data,” that can be recorded and/or stored. For most remote communications, the most secure and confidential method remains the telephone.

If an online meeting is necessary or warranted, then companies should select a service that has end-to-end encryption. This type of encryption is a security solution that prevents data from being read or modified by anyone other than the sender or recipient(s)—because only the sender and recipients have the keys required to decrypt it. One recent criticism of the Zoom platform is that its meetings are not truly end-to-end encrypted. For a complete understanding of Zoom's encryption methods, click here. However, many online meeting programs offer true end-to-end encryption for online meetings and any data shared during those meetings.

In addition to keeping online meetings secure while they are taking place, companies should also maintain and follow internal guidelines with respect to whether online meetings are recorded and/or stored. Many of the online meeting programs have the ability for users to record audio, video, and screen sharing activity, and some even offer automatic transcription of the recordings as a feature of the service. Typically, recording features and preferences must be enabled by the organizer before the meeting begins. If an organizer plans to record all or portions of the online meeting, notice should be provided, and permission obtained from all participants in the meeting before it starts.

Recorded online meetings become "Electronically Stored Information" (ESI) that may be subject to disclosure to opposing parties in litigation through eDiscovery requests. Just like emails, spreadsheets, and other electronic data, recordings of online meetings will only be protected from disclosure if they fall within one of the privileges provided for in the applicable discovery rules—such as the attorney-client communication or attorney work product privileges. However, these protections are usually very limited and may not apply to a recording of an online meeting where no attorney participated, or legal advice was provided. It is important to remember that online meeting recordings that are stored by a company should be maintained, preserved and/or destroyed in accordance with company policies and procedures governing the storage of similar electronic files.

This article **was written for Business 2 Community** by Gina Vitiello.
Learn more about writing for B2C

Author: Gina Vitiello

View full profile ›