U.S. Legal Support's Chief Information Officer, Lee Wielenga, answers 5 pressing questions regarding Zoom and its use in facilitating remote depositions for U.S. Legal Support clients.

1. Are recent media stories correct claiming that Zoom rooms can be hacked and uninvited individuals can "Zoombomb" a meeting?

Only scheduled participants can attend a meeting if identity information is properly managed. The issues reported in the media are due to meeting information being disseminated in an insecure manner. At U.S. Legal Support (USLS), all Zoom room scheduling is managed through a custom interface presented by our partner, Remote Counsel. A unique link, with a unique passcode, which is valid only for the specific Zoom room being scheduled, is sent to all participants. The room cannot be accessed until just prior to the start of the meeting and the link expires on the day the meeting has completed. In addition, only one meeting is scheduled per reserved room per day.

2. Are the stories in the media about Zoom sending privacy information to third parties without consent, as alleged in the lawsuits that have been filed in California, accurate?

The California lawsuit(s) recently reported in the media are based on reports that Zoom had included a set of code from Facebook that allowed users to log in to the Zoom iOS app (apps on iPhones and other Apple mobile devices) using their Facebook login credentials. The Facebook code allegedly sent information about the user and the device they were using to Facebook without Zoom asking for consent from the user. Zoom has reaffirmed their commitment to protecting user privacy and has ensured that current versions of the Zoom Client product do not send user data to third parties. The USLS implementation of Zoom via our partner, Remote Counsel, does not ask for or allow clients to log in to Zoom using Facebook credentials or any other credentials from third party identity providers.

3. I recently read that Zoom recordings can be accessed on the internet and are not secure. Is this accurate?

Unsecured Zoom recordings available on the internet were created by Zoom meeting participants that have recorded meetings and saved those recordings without properly securing them as per Zoom recommendations. USLS recordings are scheduled and administered by USLS hosts. These recordings are encrypted and stored on Zoom's secure platform. Recordings by individual participants other than the USLS host are not permitted. A link is made available only to parties to the matter that have also ordered a certified copy of the transcript.

4. Does Zoom support end-to-end encryption for video conferencing?

Zoom is encrypting two separate modes of data transport during a scheduled USLS meeting conducted on the Zoom platform via our partner, Remote Counsel. One is the transfer of chat text and documents transferred via the Zoom chat function. All data transferred through the chat function in a scheduled USLS meeting is end-to-end encrypted using TLS 1.2 with AES 256-bit encryption. Audio and video transferred over the Zoom platform is transport encrypted, which means that while the data is encrypted, it is not encrypted from end-to-end. Note that this is not uncommon for many conferencing platforms and is the same encryption level all internet users have when conducting secure transactions on the internet using HTTPS, including on banking platforms. Note that when Zoom passes audio data to your phone company, like all conferencing services, the data will no longer be encrypted.

5. I heard from someone that Zoom is irresponsible and not a good software platform to use for conferencing. Could you please address?

As a general statement, Zoom is experiencing an explosive level of growth due to the current health concerns that are changing the work habits of many companies, and greatly increasing the use of software that enable staff to work remotely. Zoom is a leader in this realm as their product is easy to use and feature rich. Zoom is in the spotlight now due to the millions of new people using their platform. There is a level of hyperbole in the media regarding Zoom security issues that is not fairly representing the product or how software companies that create complex software manage their products.

All complex software will have bugs, and a company should be judged on how these issues are addressed, and not on security perfection. Zoom has publicly committed to addressing any security issues raised by the reputable IT security community and has paused all new feature development for 90 days while they review issues that have been raised to ensure this commitment to security is fulfilled.

A good example of a company addressing legitimate security issues is Microsoft, who is a leader in software security and is frequently used by United States government agencies to process, transport, and store data. Microsoft has many security bugs reported every month that they address and patch. Please reference Microsoft's posting regarding their patched security issues using the following link: https://portal.msrc.microsoft.com/en-us/security-guidance