TECHNOLOGY CORNER

Privacy Settings for Zoom Video and Alexa

CHRISTOPHER B. HOPKINS

In March 2020, as professionals worked from home due to COVID-19, Zoom video conferences surged in popularity while, conversely, lawyers cast weary glances at the Alexa device in their home office, wondering if it was recording confidential communications.

As of this writing, rumors abound on social media about the security of both platforms. With little hard evidence, a BigLaw firm publicly broadcast its ban on these devices. While society struggles with its relationship with ubiquitous communication devices, let us at least properly configure our Zoom and Alexa privacy settings.

Zoom Video: Recommended Settings

As a brief primer, Zoom throws a few numbers at you which can be confusing. A Personal Meeting ID (PMI) is a virtual room assigned to you alone; this is visible on the URL, called a Personal Link, when you invite someone to your personal meeting room. Your Meeting ID is a temporary number for a scheduled meeting. The Meeting ID typically expires after your meeting unless you create a recurring meeting. These links and IDs may be confusing but the important point is that, without proper precautions, they can be hacked, re-used, or simply guessed by third parties.

The first rule of Zoom meetings is to avoid "zoom bombing" uninvited guests who disrupt the meeting by sharing pornography and malware or who simply lurk to obtain confidential information. Follow these steps to block uninvited attendees:

Password-Protect Your Meetings - Under Meetings / Schedule a New Meeting, tick the "require a meeting password" which then sends to participants the password along with the Meeting ID.

Kick Them Out - Under "Manage Participants" on the desktop and "Participants" on iOS, you can mute and remove participants.

Lock the Meeting - Once all participants arrive, lock the door behind you. On the desktop, select "manage participants," then "more," and check "lock the meeting." On iOS, hit "more" and then, under "Meeting Settings," lock the meeting.

Is This Being Recorded? - Zoom reports that all participants will see a red notification (upper left on desktop and upper right on iOS) if the meeting is being recorded.

Only the Host Has Certain Abilities - On the website, go to Settings and turn OFF "Join Before Host," "Use Personal Meeting ID," "Annotation," "Remote Control," and "Allow Removed Participants to Rejoin." Meanwhile, turn ON "Allow host to put attendees on hold" and "host only" under screen sharing.

Hypervigilance Against Zoom-Bombing- To really lockdown meetings, on the website, turn off "Join Before Host" and "File Transfer" but turn on "Require Password for… Phone" and, towards the bottom, turn on "Waiting Room." You will need to Google how to use Waiting Rooms.

The following steps will assist in protecting your privacy during a Zoom meeting:

Spacebar To Mute - press and hold spacebar to temporarily mute yourself.

Set a Virtual Background - The benefit of a virtual background is that participants cannot see the room behind you, whether that includes privileged information on a wall calendar or… a snoring pug. Select a high definition shot of the Enterprise, the Black Lodge from Twin Peaks, or (more boring) your firm's logo. On the desktop app, go to Settings / Virtual Background. On iOS, hit "more" in the upper right corner and select virtual desktop. Check out Unsplash.com and Modsy.com for background options.

Am I Being Recorded? - By default, Zoom conferences can only be recorded by the host however, keep in mind, just like someone can take a screenshot of a SnapChat, they can screen capture or otherwise record their computer without you knowing.

Really Concerned about Privacy? - According to The Intercept, Zoom is not truly end-to-end encrypted and it is definitely not encrypted if someone can attend by phone. If all participants will use Zoom and not the phone, increase your privacy when scheduling a new meeting by changing Audio to "computer audio" and not "both."

Look Your Best - While not strictly a privacy issue, on the desktop app, tap the cog wheel, then video, then Touch Up My Appearance. On iOS, select "more," then Meeting Settings, and turn on Touch Up My Appearance.

Alexa: Recommended Settings

According to Amazon, "you'll always know when Alexa is recording… because a blue light indicator will appear or an audio tone will sound…" What is less clear is what third parties are doing with your data or if voice apps have the power to control the microphone.

What Has Alexa Heard? - In the Alexa app, tap the three lines in the upper left corner and then go to Settings / Alexa Privacy / Review Voice History. Scroll through (and delete) the recent commands she recorded.

Set Up Delete By Voice Command - Following those same steps, toggle on "Enable deletion by voice." Then later you can instruct Alexa "delete what I [just said][said today]."

Auto Delete Old Recordings - Follow the same instructions but choose Manage Your Alexa Data and set auto delete to either after 3 or 18 months.

Turn Off "Use Voice Recordings to Improve Amazon Services" - Again, using the same steps, go to "Manage Your Alexa Data" and slide that option off.

What Just Happened? - If Alexa ever acts strangely, you can always ask, "Alexa, tell me what you heard" or "why did you do that?"

Alexa, who wrote this article?

__Christopher B. Hopkins__ is a cybersecurity lawyer with McDonald Hopkins LLC. He can be reached at __chopkins@mcdonaldhopkins.com__ and __@cbhopkins__ on Twitter.