**Privacy and Security Concerns about Zoom**

**Last Updated: April 3rd, 2020**

**\*\*\* The University of Toronto provides a number of institutionally supported solutions for online meetings and collaboration that have little to no additional costs associated with them, and have been reviewed for their privacy and security in various settings (but not for clinical data). A list of these tools can be found here (**[**https://act.utoronto.ca/enterprise-video-conferencing-video-meeting-resources/**](https://act.utoronto.ca/enterprise-video-conferencing-video-meeting-resources/)**). \*\*\***

While Zoom is not an institutionally supported solution at the University of Toronto, it remains a popular tool that is seeing significant use. A number of recent articles have appeared regarding the privacy and security of Zoom, and a summary of important considerations has been prepared to ensure awareness for those who choose to use Zoom for their purposes.

*If you are intending to use Zoom, please review these considerations.*

1. **Confidentiality** - The only time meetings are fully encrypted are when ALL participants are using the Zoom client AND the meeting is not being recorded. In some instances it is technically possible for Zoom to see the “Customer Content” (i.e. video, audio, chat, data/files that you may show). This risk is mitigated by Zoom’s Privacy Policy that states, “Zoom does not monitor or use customer content for any reason other than as part of providing our services.  Zoom does not sell customer content to anyone or use it for any advertising purposes.*”*.

***If you are concerned about Zoom being able see your “Customer Content” (and possibly being compelled by foreign governments to see it), then you should not use Zoom.***

1. **Your data may leave Canada** – Zoom may transmit your “Customer Content” through geographic regions outside Canada, as it uses a number of global data centres to provide its service. Zoom may attempt to use data centres that are geographically closer to where your participants reside, or use alternate data centres to help improve the quality of transmission if certain data centres are not performing well.

If you choose to record your sessions and store them via the cloud option then this data may be stored outside of Canada, quite possibly in the USA and therefore subject to their laws around who can access it.

***If you are concerned that about your “Customer Content” leaving Canada, you should not use Zoom.***

1. **Meeting security** – Zoom’s popularity has increased in large part due to its ease of use and how easy it may be to join a meeting. New types of attacks have arisen called Zoombombings that allow unauthorized users to join meetings and show inappropriate/offensive materials. Zoom has a number of security features to prevent this, the tradeoff being this may require more actions by participants to join the meeting (e.g. entering a password).

A summary of settings can be found in the document, “Default settings set in Zoom to minimize security and privacy risks”.

***Users hosting Zoom meetings should be familiar with the options that may affect the security of their meetings and the privacy of its participants.***

1. **Security Flaws and Bugs** – like any software application bugs and flaws may exist in the Zoom software and are periodically uncovered. Some are minor and some have the potential to be serious. On April 1st several serious issues with the Zoom software were announced. The following day a fix was released, and all hosts and participants will need to update their Zoom client to install the fix. It’s always a good practice to keep your Zoom client (and any software for that matter) up to date to have it patched against any known bugs or security flaw.

**Hosts and participants should ensure the Zoom client they are using remains up to date.**

**Default settings set in Zoom to minimize security and privacy risks**

**Last Updated: April 3rd, 2020**

The following settings have been defaulted to help minimize the security and privacy risks associated with using Zoom. We recognize that these default settings may not work in all contexts (e.g. having the waiting room to admit 250 learners), and have attempted to select the options that work for the majority of cases. It is possible for hosts to adjust these settings manually for their meetings – it is up to the host to decide what is appropriate given the context of their meetings.

**Meeting settings**

1. Require a password to enter the meeting
2. Screen sharing is set to host only
3. Attention tracking is set to off
4. Waiting room is set to on by default so that the host must admit users
5. Allow users to contact Zoom’s support via Chat

**Recording settings**

1. Allow hosts to record meetings locally (i.e. on their computer)
2. Allow hosts to record meetings to the cloud (i.e. on Zoom’s servers)
	1. Records the active speaker with shared screen
	2. Records an audio file
	3. Saves chat messages
	4. Display participant’s names in recording
	5. Record thumbnails when sharing
3. Automatic record is set to off
4. Only the host can download cloud recordings
5. Host can delete cloud recordings
6. Ask participants for consent when a recording starts

**Phone settings**

1. Phone numbers are masked in the participants list (e.g. they will show up as 888\*\*\*\*123)

**Best Practices for Zoom meetings**

**Last Updated: April 3rd, 2020**

1. Ensure your meeting titles do not inadvertently convey confidential or sensitive information
2. Require a password for meetings
3. Ensure your sharing options are appropriate for your meetings. The default is set to only the host may share
4. Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.
5. Minimize any personal information exposure – encourage participants to log in using only their first name and last initial
6. Ensure participants provide their consent to being recorded
7. Keep your camera and microphone off unless you’re speaking
8. Do not ask users to sign up for Zoom with a personal email address – always use an institutionally provided email address