Privacy and Security using Video Meeting Software

Like most online data collection tools, the use of video conferencing software comes with certain risks. The primary risk associated with online video tools is of intrusion or access by unauthorized parties. In most cases, risks to participant privacy can be mitigated by applying settings that keep data held as locally as possible and viewable by only authorized parties.

In all cases, participants should be made aware of the tools used to gather data and the associated risks. Researchers using Google Meet, Zoom, or similar software to gather data should include the following statement in letters of consent:

> Your information will be collected using [software name and company location]. The information you submit may be subject to laws in force outside of Canada. As with any information transmitted via the internet, there is some risk that data may be intercepted by unauthorized parties and, therefore, privacy cannot be absolutely guaranteed.

Researchers who will be shifting in-progress projects to an online environment may need to modify ethics applications and re-consent participants. Please contact hreb@mtroyal.ca for guidance if this applies to you.

Phone

Consider using your phone to conduct remote research. Phone calls are generally more secure than video meetings. There are numerous apps available for smartphones that facilitate phone call recording. When possible, ensure that recordings are stored on your phone and not automatically uploaded to cloud storage.

Google Meet

Meet is the preferred video meeting software for regular University business. Google uses security protocols that are compliant with international standards. Video data using Meet is encrypted in transit between each user and Google servers, which act as nodes to connect participants in a virtual meeting. While Google does operate data centres in Canada, complete data sovereignty is rarely guaranteed for software that operates internationally.

Meetings can be recorded by the meeting organizer or by meeting participants from the same organization. **Regardless of who initiates the recording, recordings are appended as video files to Google Calendar Meet invitations; anybody with access to the Calendar invitation can view the recording**. If the meeting organizer initiates the recording, the video will be uploaded to their Google Drive account. If a participant initiates the recording, the video will be uploaded to the organizer’s account and automatically shared with the participant.

For this reason, researchers should not use Google Calendar invitations to set up confidential Meet conferences that will be recorded. For greater privacy, researchers should establish a meeting time with participants by other means, create a Google Calendar conferencing event *without adding guests*, and forward the meeting URL to participants. Researchers themselves should initiate the recording. For sensitive research, video files should be downloaded as soon as possible to a local device and deleted from the researcher's Google Drive account.

Zoom

Like Google, Zoom operates data centres in Canada, a practice that supports but does not guarantee data sovereignty. Zoom encrypts data travelling between video conference participants and its servers, but there is some evidence that the encryption methods used by Zoom are not as secure as they could be, and there may currently be a security issue with Zoom's waiting room feature.

Some concerns have been raised about unauthorized access to Zoom meetings, or "zoombombing." This type of access can be prevented by using adequate security settings when hosting meetings. Zoom has made recent changes to its software that default to more secure settings.

If you are using Zoom for research, familiarize yourself with both online account settings and meeting controls. Key considerations for settings and controls include:

1. When hosting a meeting using Zoom, do not use your Personal Meeting ID. Instead, allow Zoom to generate a meeting ID and password that you can share with your participant(s)
2. Require participants to sign in before they can join the meeting
3. Prevent participants from joining prior to the host
4. Once all expected participants have joined, lock the meeting
5. Save recordings directly to your personal computer

Jami

Jami is an open-source alternative to Meet or Zoom. Jami is not as feature-rich as other software, but is relatively secure. Unlike Meet and Zoom, which connect meeting participants via central servers, Jami connects users directly with each other when possible using industry-standard end-to-end encryption.

Jami meetings can be recorded, with local device storage being the only option. Participants must install the software or app, which is available for all major platforms, including mobile devices.

Summary

All three tools are suitable for most research, as long as participants are made aware of the small risk of unauthorized access.

For very sensitive research, Jami is the most secure of the three, though it is not as user-friendly. Google Meet is a secure alternative but users must be aware of its settings and ensure that recordings are not inadvertently shared. Recordings should be downloaded to local devices and deleted from Google accounts as soon as possible following meetings.