SFU

Interviews on *Zoom 5.0*

Ethical Considerations + Best Practices

Zoom's Privacy Policy

- Does not monitor your meetings nor its contents
- Does not and has no intentions of selling user's data
- Complies with privacy rules/laws (incl. FIPPA, GDPR & CCPA)

There is currently **no full end-to-end encryption**.
Audio & Video data sent through Zoom are encrypted, but keys are generated and held by Zoom (as of May 7, 2020).

US Privacy Laws

The **USA Patriot Act (2001)** and **Cloud Act (2018)** supersedes the *Zoom Privacy Policy* security provisions by making it possible for US federal law enforcement to compel US companies to provide data stored on their servers. Just because *Zoom* states that they do not monitor your meetings, this does not mean that they are not collecting such data (IP addresses, operational data, and user interactions).

These laws apply to cloud storage services **Dropbox, iCloud, OneDrive**

What you can do

Store Data Locally

Change your default Zoom 5.0 settings so recordings are stored locally instead of uploaded to a US-owned cloud service.

Settings » Recording » File location

Alternative Cloud Storage: SFU Vault
All SFU Faculty, staff and students with active SFU Computing ID are offered 50 GB.

Informed Consent

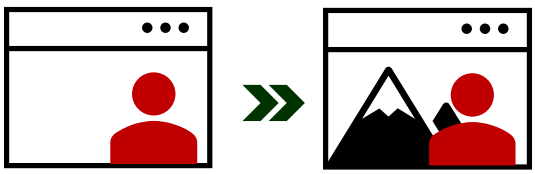
Your consent documents must alert participants that their data is subject to U.S. privacy laws.

Suggested Wording for Consent Process

"This interview is hosted by Zoom, a US company, and as such, is subject to the USA Patriot Act and CLOUD Act. These laws allow government authorities to access the records of host services and internet service providers. By choosing to participate, you understand that your participation in this study may become known to US federal agencies."

Ask Before Recording

Ask participants if they are comfortable being recorded (audio and/or video). If you are video recording, tell them about virtual background options.



Created by Vienna C. Lam | For more information, please contact dore@sfu.ca

v. June 2020

SFU

Interviews on *Zoom 5.0*

Ethical Considerations + Best Practices

Interview Preparation

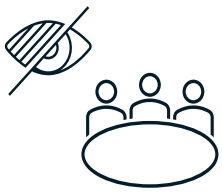
SFU IT advises researchers to use their SFU Institutional Zoom accounts.

Participant Call Setup

- ❑ SFU institutional Zoom accounts will show the participant's full name unless they create an alias for the meeting. Explain how they can change their name or provide a research code ahead of time.
- ❑ Explain how participants can turn off their camera and mute their microphone as preferred.
- ❑ Zoom has been criticized for re-using the same meeting IDs, so lock your meetings (default does not require passwords) to block intruders.
- ❑ Enable waiting rooms to screen attendees.

Group Interviews

- ❑ If the session is being recorded, notify participants that there may be limitations on the withdrawal process (i.e., post-production editing, audio files collecting all voices, etc.).
- ❑ As the host, disable recording options for participants and ask all participants to not use other recording services.
- ❑ Discuss risks as appropriate, given that there are no effective means of stopping participants from using third-party recording software.



General Tips

Avoid collecting what you do not need.
Delete audio recordings after transcription.
Password protect/encrypt your files and folders.

Additional Resources

SFU IT Services: https://www.sfu.ca/itservices/remote-study-work-resources.html
The Electronic Frontier Foundation: https://www.eff.org/

Created by Vienna C. Lam | For more information, please contact dore@sfu.ca

v. June 2020