Video Conferencing and Consent Guidelines

Summary

The use of online/virtual communication platforms carries privacy risks that researchers need to consider when designing their studies. They should only be used where the risk to participants is considered 'low' or 'moderate' should data inadvertently be disclosed. This applies to any platform (eg. Zoom, Facetime, WhatsApp, Skype, MS Teams, Jitsi, etc.) Consenting processes should make the potential risks to participants clear, and offer alternative methods for data collection should participants so wish.

Guidance

It is difficult to guarantee the security of any online communication platform, and looking for phrases like 'encryption' in terms of service can be misleading because many services offer partial, but not complete encryption of traffic, and the way that this is described can be very confusing (or misleading). Language around the storing of logs of communications can also be very confusing. Researchers should also be aware that most platforms will allow any participant to capture or record the contents of a communication in real time, which potentially introduces a further risk. This is of particular concern for focus groups conducted via a video-conferencing platform as a participant could record the information being provided by other participants.

Currently, McMaster University has institutional subscriptions for MS Teams, Zoom and Webex. Some faculties have subscriptions with other providers such as Vidyo. Institutional subscriptions offer certain protections to members of the McMaster community that are not present with services for which there is no institutional subscription. Therefore at this time, we recommend the use of MS Teams, Zoom and Webex for research activities which involve remote video communications. The choice of platform can be based on preference.

It is important to note that none of these platforms (nor any other online meeting platform) should be considered 'fully secure'. Their use would be considered appropriate for low and medium risk studies, where the risk to participants should the contents of interviews be released is considered 'low' or 'moderate'. If the risk is high, such data should be collected via face-to-face interviews or by an encrypted voice calling or messaging service such as 'Signal' which has clear policies about the storing of logs of communication metadata.

Consent forms should include language that makes it clear what platforms are being used, and also that no guarantee of privacy of data can be made, so the risks of participation are clear. Example language might be ***"This study will use the X platform to collect data, which is an externally hosted cloud-based service. A link to their privacy policy is available here (LINK). While the Hamilton Integrated Research Ethics Board has approved using the platform to collect data for this study, there is a small risk of a privacy breach for data collected on external servers.***

***If you are concerned about this, we would be happy to make alternative arrangements for you to participate, perhaps via telephone. Please talk to the researcher if you have any concerns*."** Consent forms should also include language that participants agree not to make any unauthorized recordings of the content of a meeting / data collection session, and in the case of focus groups remind participants that researchers cannot guarantee that all participants will refrain from recording the session.

Unless video is required for data analysis the recording should be of audio only, and the consent form should specify what is being recorded (audio only or both audio and video). Similarly, unless seeing the participant(s) via video is essential to the data collection methodology, the participant(s) should be given the option to participate in the meetings by audio only. When making recordings, it is important that they are saved to a local computer rather than to the cloud-based service.

For more information about the Zoom, Webex, and MS Teams platforms, please see here:
https://cto.mcmaster.ca/zoom-video-conferencing-best-practices-for-privacy-and-security/

https://research.mcmaster.ca/videoconferencing/zoom/
https://research.mcmaster.ca/videoconferencing/webex/
https://research.mcmaster.ca/videoconferencing/msteams/

The above information is courtesy of McMaster University (McMaster Research Ethics Board, IT Security, Office of the VP Research).