Participants (and bots) falsifying their identity

Summary

Researchers may find themselves engaged with participants who appear to have falsified their eligibility in order to receive remuneration from participating in a study. Researchers may also have cause to suspect that some responses to their surveys have been generated by a malicious element such as a bot.

When a research participant's identity is called into question, the integrity of the data and the data of other participants is called into question. The researcher loses data and time and incurs costs associated with remunerating falsified participants. The Behavioural Research Ethics Board was asked for advice on how to prevent this occurrence, and to describe what approaches would be ethically acceptable when a researcher believes a participant has falsified their identity. The purpose of this document is to raise researcher awareness and provide potential solutions that would be acceptable from a research ethics perspective.

Researchers have reported situations where a participant claims to be part of the selected demographic but where a mismatch becomes apparent during an online interview, asynchronous chat or other engagement, e.g.:

- Claims to be a parent of an adolescent or young adult but being too young for this to be feasible
- Claims to live in the required geographic area but doesn't have appropriate contact information or changes their details after participation begins
- Claims to have a qualifying medical condition, such as dementia or other illness, but then supplies details that don't match their pre-screen answers
- Evidence emerges that an individual (IP address) has enrolled multiple times under different names
- Claims technical problems (with Zoom or other interface) when asked knowledge questions
- Asks to replace an online interview with a (text-based) chat.

Social media recruitment and online participation options increase the likelihood of falsification.

Creating secure online surveys

You may encounter "bot-like" response behaviour in online surveys. Bots are difficult to identify, but a number of anomalies may help, such as unknown email address domains, repeated or patterned survey responses, and unusual time to complete the survey. Advanced Research Computing (ARC) recommends the following when using online surveys:

- Avoid sharing survey links on publicly accessible platforms (such as social media) unless your aim is to generate a very large number of responses.
- Where possible, limit the number of responses a single participant can submit, as well as time to complete the survey.
- If survey access is shared via email, configure the survey link to only allow invited participants to access the survey and ensure the link is set to expire after a specified amount of time.

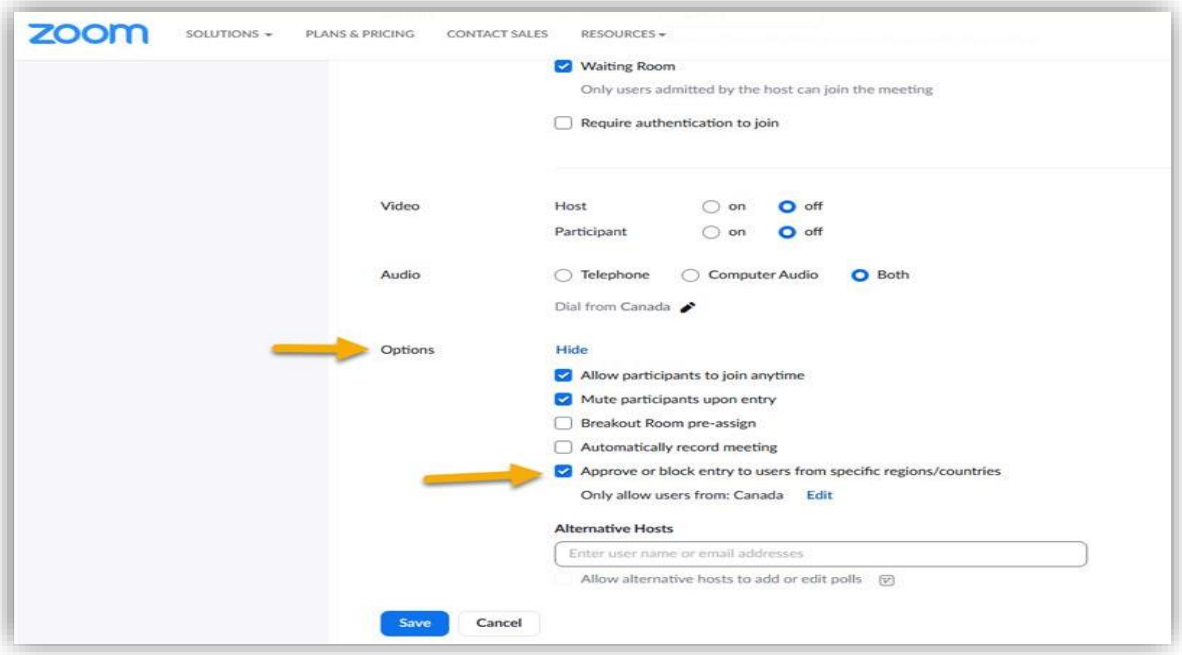
- When using Qualtrics, security features such as bot detection, multiple selection prevention, relevant ID and security scan monitor feature (see Survey options/Security) may help protect researcher's survey data integrity. For detailed information, see https://www.qualtrics.com/support/survey-platform/survey-module/survey-options/survey-protection/.

Social media recruitment and online participation options increase the likelihood of falsification.

Ethically acceptable mitigation steps

Since the offer of remuneration seems to be the reason that participants falsify their identities, the solutions provided below focus on changing how identities are validated, and how remuneration is offered. The approaches will not guarantee that participants don't continue to falsify their identities, but they will hopefully dissuade some and allow for earlier detection of others. Most of the suggestions will need to be recorded in the consent form so invitees have the necessary details to make an informed decision about consent.

1. In social media recruitment ads:
   - Where applicable, do not advertise how remuneration will be offered, or include that remuneration will be in the form of **Canadian** gift cards (i.e. that cannot be cashed in globally) or. Orient research staff on how to answer questions from potential participants that are purely about method of payment.
   - Indicate that use of video will be required to confirm the identity of participants.
2. In consent forms:
   - Where video will be used to confirm the participant's identity, indicate that only those who are able to use the specified technology will be able to participate. Be clear in the consent form how a participant's identity will be verified; e.g., by asking to see (without recording) their driver's license or other identification; or just through informal facial recognition.
   - Where the current residence of the participant is an inclusion criterion, state that the gift card/remuneration will be mailed to participants and ask for their mailing address.
     Depending on the level of confidentiality being promised, the addresses may need to be stored separately from the participant's responses, and destroyed after remuneration is complete.
   - Where possible, avoid using gift cards or vouchers that have worldwide usage; e.g., use gift cards from a Canadian retailer, and specify the source of remuneration in the consent form.
3. For interactions on Zoom, ask that participants start the session with their video turned on (so the interviewer can verify identifying details).
   - It is possible when setting up a Zoom session to limit participation by geographic area (see screenshot).



4. For asynchronous chat discussions or in online interviews:
    - Include pre-screening questions and/or embed questions about the participant's demographic information, whereby those who do not answer correctly are removed.
    - Have a plan for dealing with participants who have falsified their identities and disclose in the consent form. For example, "If you do not pass a short pre-screening questionnaire to confirm your eligibility, you will not be compensated and will be removed from the study."
5. If a participant has to be disqualified, the researcher may still need to reimburse them for a portion of their time depending on what was agreed to in the ethics application and stated in the consent form. When in doubt, a participant should be compensated. Research staff should be instructed to avoid making accusations.
6. Ensure that the research team staff are introduced to the possibility of participants falsifying their identity and provide instructions for discontinuing an interaction if necessary and for discarding data.

Final notes

Constraints placed on participants to qualify for a research study must be disclosed in advance, usually through recruitment and consenting steps.

Researchers are advised to avoid technical requirements that might create stigma, cause distress, or place an undue burden on a population, e.g., by disqualifying those who may be struggling with technology due to health or other issues.