the british psychological society
promoting excellence in psychology

Ethics guidelines for internet-mediated research

REPORT

June 2021

AUTHORS

These guidelines were originally prepared by the Working Party on Internet-mediated Research, convened under the aegis of the British Psychological Society's Research Board in 2014. The guidelines were reviewed in 2017 and again in 2020–2021. Below are the members of the respective review panels.

2017

DR CLAIRE HEWSON (EDITOR AND CONVENOR)

PROFESSOR TOM BUCHANAN (EDITOR)

DR IAN BROWN

DR NEIL COULSON

DR GARETH HAGGER-JOHNSON

PROFESSOR ADAM JOINSON

DR ALEKS KROTOSKI

PROFESSOR JOHN OATES

2021

DR LINDA K. KAYE (CHAIR)

DR CLAIRE HEWSON

PROFESSOR TOM BUCHANAN

PROFESSOR NEIL COULSON

DR DAWN BRANLEY-BELL

DR CHRIS FULLWOOD

MS LAURA DEVLIN

ISBN: 978-1-85433-796-2

Contents

Executive summary

Internet-mediated research (IMR) can raise particular, sometimes non-obvious, challenges in adhering to existing ethics principles. In this document we outline some of the key ethics issues which researchers and research ethics committees (RECs) are advised to consider when implementing or evaluating an IMR study. Regarding each of the four main ethics principles as outlined in the Society's *Code of Human Research Ethics* (2021), we highlight issues which may need special consideration in an IMR context, using illustrative examples to explain why. These issues include: the public-private domain distinction online; confidentiality and security of online data; participant anonymity, procedures for obtaining valid consent; procedures for ensuring withdrawal rights; levels of researcher control; and implications for scientific value and potential harm of both participants and researchers.

Emphasis throughout is on offering advice on how to think about and apply existing ethics principles in an IMR context, while recognising that issues need to be assessed and decisions made within the context of a particular piece of research. Given the diversity of IMR methods, this document should not be perceived as a comprehensive 'how-to' guide for conducting online research, but rather as a reference point for helping researchers to appraise key considerations and make decisions when designing projects which use the internet to gather data.

Introduction

This document presents guidance on how the *Code of Human Research Ethics* (BPS, 2021) may be interpreted in the context of Internet-mediated research (IMR) and what special considerations may apply. It should be considered as supplemental and subordinate to the Society's *Code of Human Research Ethics* (2021) and the overarching *Code of Ethics and Conduct* (BPS, 2018). It closely follows the principles and advice offered there, highlighting areas where these may become problematic and require particularly careful consideration in an IMR context.

The primary function of this document is to help researchers and research ethics committees (RECs) plan and evaluate research proposals, and to help with the process of ethical decision making in the context of specifying and implementing appropriate IMR research designs. It is not intended to provide a 'rulebook' for IMR. It should be recognised that technologies, their social uses and the associated implications for research may change rapidly over time and new considerations will become salient. This requires a return to 'first principles' and an informed application of general ethics principles to the new situation. This document deals with some of the issues one may need to think about.

The *Code of Human Research Ethics* (BPS, 2021) outlines the four main principles underpinning the ethical conduct of research:

- respect for the autonomy, privacy and dignity of individuals and communities;
- scientific integrity;
- social responsibility; and
- maximising benefits and minimising harm.

Internet-mediated research

Advances in technology and Internet connectivity extend opportunities for psychological research. Such technological advances may also introduce additional, and sometimes non-obvious, complexities relating to interpreting and applying ethics principles. This is particularly true in the case of internet-mediated research (IMR).

IMR covers a wide range of quantitative, qualitative and mixed methods approaches to research involving, or about human participants. It can be broadly defined as any research involving the remote acquisition of data from or about human participants using the Internet and its associated technologies. As with traditional approaches, IMR projects may adopt a variety of research designs. Their focus may be on obtaining quantifiable measurements or garnering rich, elaborate narratives, through qualitative approaches. They may be reactive where participants interact with either the materials and/or a researcher (e.g online surveys, online interviews). Alternatively, they may be non-reactive where data about individuals are collected unobtrusively from secondary sources which were not created as part of the research (e.g. analyses of social media postings, interpersonal social network links, or other types of online activity such as search engine histories or digital traces stored as a by-product of smartphone app usage).

The boundaries between IMR and other designs can be blurred where research includes elements of both in-person* observation/interaction and remote data collection. However, the key point is that the design normally involves acquisition of data from or about individuals in the absence of physical co-presence. This restricts the researcher's capacity, in contexts where a participant is actively aware of and knowingly participating in a study (i.e. reactive contexts) to monitor, support, or even terminate the study (e.g. if adverse reactions become apparent). Even in contexts where researchers can monitor the reactions of their participants (e.g. via video chats), consideration may need to be made about how communication dynamics might be different and in some way impoverished compared to in-person settings (e.g. some may find it more difficult to build a rapport or read the reactions of others because nonverbal communication cues can be absent or attenuated). These key features of IMR can raise a number of ethics issues which need careful consideration. Additionally, very often research participants will be located in one or more different countries, so a project may span multiple nations, cultures and legal jurisdictions. Care should be taken when designing research to ensure that if online methods are being used, especially if these are attempting to substitute in-person designs, that this format is appropriate. Most research paradigms may require specific modifications to ensure these are appropriate and effective online.

Different types of IMR design raise different ethics considerations. While many of these issues are detailed in the *Code of Human Research Ethics* (2021) and are not unique to IMR, in this context they may create special considerations regarding the way the general principles should be interpreted and applied. For example, the extent to which the research can be thought of as occurring within a private or public domain, may be difficult to decide, given that those boundaries are often blurred online.

As noted above, level of risk to participants may be difficult to monitor and control in some IMR designs, given researchers' lack of direct oversight over participants' behaviour, mood or identifiability. This, along with the ubiquity/accessibility of the Internet and the data on it, may have implications for procedures

* 'In-person' or 'offline' is used throughout this document to refer to activity which takes place in non-online settings. This term is used instead of more typical terms such as 'face to face' as it is becoming increasingly accepted that using online platforms such as video-calls can largely resemble 'face to face' interaction.

for ensuring valid consent, withdrawal, as well as protection of participants. Additionally, emerging new methods may give rise to novel ethics issues, and this point should be kept in mind when considering the novel methodological opportunities afforded by IMR. Particularly, this can include the emerging use of AI/machine learning algorithmic approaches in social and behavioural research, facilitated by the enhanced prevalence of big data sets now readily available online (e.g. from social media sources). These can lead to inferences and predictions being made about individuals (and/or groups) that go beyond the information readily apparent to a human observer. Although it is beyond the scope of this document to delve into the details of these techniques and issues in any depth, researchers should be aware of the emerging use of these approaches to understand human behaviour.

A summary of the main ethics issues for researchers and RECs to consider when designing, implementing or assessing an IMR study can be found in Table 1.

TABLE 1: SUMMARY OF THE MAIN ETHICS ISSUES TO CONSIDER WHEN DESIGNING, IMPLEMENTING OR ASSESSING AN IMR STUDY

Principle	Considerations
Respect for the autonomy, privacy and dignity of individuals and communities	*Public/private distinction* – The extent to which potential data derived from online sources should be considered in the public or private domain. *Valid consent* – How to implement robust, traceable valid consent procedures. *Confidentiality* – Levels of risk to the confidentiality of participants' data, and how to minimise and/or inform participants of these risks, particularly where they may potentially lead to harm. *Anonymity* – How to implement robust procedures which allow participants to remain anonymous and non-identifiable. *Deception* – How to ensure participants are treated respectfully with regards to researcher disclosure and research purposes. *Withdrawal* – How to implement robust procedures which allow participants to act on their rights to withdraw data. *Copyright* – Copyright issues and data ownership, and when permission should be sought to use potential data sources.
Scientific integrity	*Levels of control* – How reduced levels of control may impact on the scientific value of a study, and how best to maximise levels of control where appropriate.
Social responsibility	*Disruption of social structures* – The extent to which proposed research study procedures and dissemination practices might disrupt/harm social groups.
Maximising benefits and minimising harm	*Maximising benefits* – How each of the issues mentioned above might act to reduce the benefits of a piece of research, and the best procedures for maximising benefits. *Minimising harm to participants* – How each of the issues mentioned above might lead to potential harm, and the best procedures for minimising harm. *Minimising harm to researchers* – How each of the issues mentioned above might lead to potential harm to researchers and/or institutions, and the best procedures for minimising such harm.

Ethics guidelines for internet-mediated research

We now consider each of the four principles, as outlined in the *Code of Human Research Ethics* (2021) and highlight issues which should be given especially careful consideration in an IMR context.

PRINCIPLE 1: RESPECT FOR THE AUTONOMY, PRIVACY AND DIGNITY OF INDIVIDUALS AND COMMUNITIES

The *Code of Human Research Ethics* (2021) highlights several key considerations related to this principle, including: valid consent, withdrawal, confidentiality, anonymity, fair treatment, and rights for privacy. In an IMR context, the issue of privacy is especially problematic and needs additional careful consideration due to the unclear status of different sources of online information which may serve as potential research data (e.g. discussion forum posts, social media site activity, app-generated data). IMR facilitates the potential collection of large data sets, including traces of people's online behaviours, some of which have ambiguous status in terms of whether they should be considered 'in the public domain' and/or readily available for use as research data (for example, without gaining informed consent).

Closely linked with privacy considerations are issues of anonymity and confidentiality. The availability of very large volumes of data online increases the possibility that linking together data sets and/or applying specific analyses (e.g. using algorithmic manipulations) could reveal (or re-identify) individuals' personal characteristics or even identities. Also related to considerations of privacy are valid consent, including when researchers should strive to ensure this has been obtained and how to properly gain it, and withdrawal; particularly, how to properly implement robust procedures for this in IMR. We now discuss these key issues related to this first principle, offering examples and illustrations.

PRIVACY ONLINE

The *Code of Human Research Ethics* (2021) notes that, unless consent has been sought, observation of public behaviour needs to take place only in public situations where those observed would expect to be observed by strangers, essentially vetoing observation in public spaces where people may believe that they are not likely to be observed. In an IMR context, the distinction between public and private space becomes increasingly blurred. For one thing, much Internet communication can take place in both a private (e.g. the home) and public (e.g. open discussion forum) locations simultaneously.

Secondly, in this continually-evolving medium it is not always easy to determine which online spaces people perceive as 'private' or 'public'; where they might be happy to be observed, or otherwise. Determining an online space as either public or private is not entirely dichotomous particularly when people's own perceptions of privacy can vary. For example, in some online spaces, users may have an expectation of only being observed by a specific audience. To complicate things further, a communication perceived as private at the time might become public at a much later date (or vice versa). This may include a post in a locked

social media account that becomes public when privacy settings are changed, or when material a user thinks they have deleted is actually retained somewhere in a public archive, for example. There are also platforms which allow users to post 'fleets' which are time-sensitive and so disappear after a short period of time (e.g. on Snapchat). While much internet communication can often be considered public through greater visibility, traceability and permanence, it is not always apparent whether this makes it ethically acceptable to use such data freely for research purposes. Opinions on this issue have varied widely, and the expectations and wishes of users, in different contexts (and by different user groups), have been unclear. This accessibility and relative permanence of the traces of people's online activities, behaviours and interactions raises issues in IMR which are not present in the same way in offline contexts which are generally more transitory. Researchers should be aware that participants may consider their publicly accessible internet activity to be private despite agreeing to the terms of the web service providers' End User Licence Agreements, or indeed that the communication may have been private when it was first conducted, even if it later becomes publicly available. Furthermore, service providers and corporations may publish data, potentially that identify individuals, that the individuals themselves had never expected or agreed would become public.

Opinions differ on whether materials posted in so-called 'public' (perhaps best thought of as 'readily accessible by anyone') online spaces (e.g. social media, discussion groups, blogs, etc.) should be automatically classed as public activity. When there is a level of ambiguity concerning whether data are 'in the public domain' or not, researchers should particularly consider likely user perceptions and attitudes, and the extent to which undisclosed observation may have potentially damaging effects for participants, before making decisions on whether to use such data and whether gaining valid consent is necessary. It is important to note that analysis of online discussions or other activities is not precluded, but it should be carefully considered in light of the ethics concerns highlighted here. A discussion group moderator or administrator may often provide a good point of contact for advice on navigating these issues, and the best ways to research existing online groups.

Where it is reasonable to argue that there is likely no perception and/or expectation of privacy (or where scientific/social value and/ or research validity considerations are deemed to justify undisclosed observation nevertheless), use of research data without gaining valid consent may be justifiable. However, particular care should be taken in ensuring that any data which may be made accessible as part of the research remains confidential (often achieved by ensuring anonymity, since dissemination of research findings is, generally speaking, inevitable) – see the further discussion of the possible threats to anonymity and confidentiality in IMR under Principle 4 below. As the chance of violations of anonymity and confidentiality that could harm participants within a given research methodology increases, arguments that valid consent is not necessary are weakened. Essentially, a key principle in IMR (as well as in offline methods) is to ensure that ethics procedures and safeguards are implemented so as to be proportional to the level of risk and potential harm to participants.

VALID CONSENT

Valid consent should be obtained where it cannot be reasonably argued that online data can be considered 'in the public domain', or that undisclosed usage is justified on scientific value grounds (as set out in the *Code of Human Research Ethics*, 2021). In these cases, valid consent would be needed. The Data Protection Act (2018) outlines that the lawful purpose of processing personal data may be applied if the exercise is deemed necessary for public interest. Assuring that the principle of participation on the basis of valid consent is fully complied with can raise particular issues in IMR. Obtaining a record of valid consent arguably requires verifying certain relevant characteristics of the person providing it (e.g. to determine that they meet any necessary age requirements). This can be more difficult to achieve in an IMR context than in situations where there is direct in-person contact with participants – see the further discussion of this point under Principle 4 below.

Establishing that participants have properly engaged with valid consent procedures in IMR is not always easy, particularly for anonymised questionnaires. As with paper questionnaires, completion of a questionnaire may often be seen as a proxy for valid consent. Provided that an information sheet describes the purpose of the study beforehand, the true nature of the questions that follow, and how the researcher proposes to process and disseminate any data/findings from the study, valid consent can arguably be assumed if the questionnaire has been completed. However, it is recommended good practice to include a designated consent page as part of an online questionnaire with check boxes (for example) in response to explicit consent statements (offered both at the start and the end of the procedure). Use of check boxes can also be an effective strategy for allowing participants to indicate that they have read and understood key aspects of the consent information (e.g. their withdrawal rights, how information will be disseminated). Counterbalancing how consent statements are worded may help encourage participants to read the information (i.e. to avoid making it easy to simply tick all boxes and proceed). However care should also be taken not to 'over complicate' consent procedures online, so that participants who do clearly wish to proceed and participate in the study can easily do so. Overly lengthy consent information pages are actually likely to be counterproductive, as they are more likely to be quickly skimmed, or not read at all.

When consent is requested, it is advisable to ensure that this includes GDPR/UK Data Protection Act (2018) privacy information too (e.g. "I understand that information will be used only for the purposes previously outlined and my consent is conditional upon the university complying with its duties and obligations under the Data Protection Act (2018)'). As in all research environments, special care needs to be taken when seeking valid consent from groups whose members may be vulnerable to coercion. Procedures (perhaps necessarily offline) will often need to be used to obtain parent/guardian consent before conducting research with underage or vulnerable participants online. For interviews or focus groups which take place online via video chat platforms, care should be taken to ensure that these have sound privacy policies regarding use of data (e.g., that data is not passed onto third parties) but importantly that researchers ask for consent both for audio and video recording should different modalities be part of any recordings.

It is important in IMR, as in any research, that participants providing valid consent are given sufficient details about the study, and the nature of their participation, as well as possible associated risks. Information relating to dissemination of data is needed as part of informed consent, especially in respect of making participants aware when data may be being publicly shared on open data repositories. Not all risks in research are obvious in IMR, as they can be different to risks that might normally be present in offline contexts. One prolific but perhaps not fully understood such risk relates to the levels of researcher control over confidentiality of data (discussed in the next section).

CONFIDENTIALITY

There are arguably more risks to confidentiality of research data using IMR than other methods, during both the data gathering and sharing/dissemination stages. For example, vulnerabilities here could be where data are stored on the server of a third-party software provider during collection, or where shared de-identified data sets may potentially become re-identified when combined with other information readily available online, or be traced back to their original source where identities may be revealed. While it is typical practice (offline) to assure participants of the confidentiality of their personally identifiable information, in IMR the risks for violating this principle can be greater, particularly where researchers are not experts in online technologies and security systems. Researchers need to be aware that it is in many cases impossible to maintain absolute confidentiality of participants' personal information gathered online because the networks or systems are not in the full control of the researcher. Situations where data are collected in IMR with no potentially identifying information attached are not common. For example, even an IP address stored alongside online survey responses may be linked to an identifiable individual (see the further discussion under Principle 4 on potential risks to anonymity and confidentiality). Furthermore, data sets that may seem entirely anonymous in themselves might include patterns of information that when combined with other data sets, and/or subjected to statistical analysis techniques, could identify individuals and link them with information, potentially of a personal and/or sensitive nature. The likelihood that participants may be: (i) identifiable through these methods; and (ii) that someone may seek to corroborate data in this way, particularly for harmful purposes is relatively low. However, it is a pertinent consideration which researchers should be aware of and take actions to reduce.

Researchers need to consider ways in which participants are properly informed about how the data they provide are electronically stored and/or transported, particularly where risks are higher (e.g. standard email is a relatively insecure transmission method, cloud-based data storage may be vulnerable during downloading and uploading processes). Further, participants should be informed about the possibilities for breaches of confidentiality through the use of search engines and the accrual of data from multiple sources (as noted above). For example, published anonymised verbatim quotes (e.g. in research papers or data repositories) may be traced to the discussion forum archives from which they originated, where they are likely to be linked to an individual's identity (discussion group posts might be permanently archived). As noted above, data sets that do not appear to contain any personally identifying information, on the face of it, might include information (e.g. patterns of activity, or responses) that can lead to identifiability if combined with other data sets (e.g. that might repeat these patterns but with identifying information also included). Researchers should be clear about the extent to which their own collecting, processing, reporting and interpretation of data obtained from the internet might pose additional threats to privacy over and above those that already exist, and whether this might expose participants to potential harm of any sort. Any additional risks in IMR may need to be conveyed to participants (particularly where these risks are higher), whilst also taking all reasonable precautions to reduce levels of risk and safeguard the confidentiality of data. Researchers are encouraged to have well-developed data management plans to fully address these confidentiality-related issues. Because these data security procedures have both legal and ethical implications, it is suggested that researchers may draw on specialist advice on these issues from governance experts in their organisation.

ANONYMITY

As noted above, issues of confidentiality and anonymity are intricately linked – the anonymising of data typically being a way of supporting confidentiality. Where data are particularly sensitive and/or more difficult to anonymise (e.g. data using detailed personal narratives) then risks to confidentiality increase. There are few occasions when researchers will require personal details such as names, but there may be other personally identifiable information garnered through IMR (e.g. location, IP address, email address). If these data are collected automatically by survey software, it is advisable that this is only used to check for multiple completions and deleted as soon as possible from data sets. Should researchers need to match participant responses over time-points or need a way to identify data for retrospective withdrawal, they should ask participants to provide a memorable code or ID number which can be used for these purposes. Where identifying information such as an email address is required; for example, to follow-up/contact participants at a later stage, or send a participation reward voucher, then researchers should strive to store these details separately from the actual study responses. This could include keeping a carefully protected code sheet (accessible only by the researcher) that can be used to link names and data sets where necessary. Here again the principle of proportionality of consent procedures to level of risk applies; where threats to confidentiality are greater, it might be argued that participants should be carefully informed of the nature of these risks. Similar considerations should also be applied in the context of sharing of full research data sets, such as when deposited in research data archives.

DECEPTION

For some research designs, it may be necessary to withhold relevant information or disguise the research question(s) before data gathering (e.g. to avoid contaminating the data and jeopardising the validity and scientific value of a study). This may arguably be seen as involving some level of deception of participants which (depending on context) can raise additional ethics concerns. In offline research, such ethics issues are typically addressed by debriefing participants about the true nature of the research at the end of the study. This respects the dignity of persons by explaining why the study was conducted in this way, and reassuring participants. In IMR there is an additional risk: that participants may not participate for the full duration of the study and may not be exposed to the debriefing information that could otherwise provide important safeguards. This can be mitigated by including important support websites or helplines in the introduction and initial briefing stages of the research, in addition to the debriefing information provided at the end.

RECs should balance the scientific value of any withholding of information or deception against the risk that participants may discontinue before the disclosure and debriefing (relatively easily done in an online survey), and any likely harm that could emerge in such cases. In cases of deception, additional mechanisms are important such as including a ‘Quit study’ button which can lead to a debrief page. This may reduce the likelihood of participants closing their browser completely and missing critical debrief information.

There may be instances where researchers make use of online communities and gather data as participant observers but do not disclose their true identity in an attempt to avoid disrupting social structures. In these cases, it is good practice to consult with administrators or moderators prior to engaging, and behave in ways consistent with the norms of that community and the ethical principles of respect for others and avoidance of harm to the community.

WITHDRAWAL

An important element of valid consent is ensuring that participants are aware of their right to withdraw from participating in research (both during the study and retrospectively). At the consent stage, this should include details about any necessary time limits on data withdrawal, and the mechanism by which participants are able to request their data is withdrawn (e.g. using contact details provided). Therefore any requests from participants to remove their data which are in accordance with these rights should be complied with. The time limit for retrospective withdrawal should not be unreasonable or aimed at restricting the right to withdraw. However, it is reasonable in cases where, for example, aggregate data may be produced, analysed and then prepared for publication. The possibility of retrospective withdrawal may also require additional mechanisms for storing large data sets in ways that would identify (to the researcher only) individual contributions to the research. This point may not be unique to IMR, but the solutions for tracing individual data that have otherwise been stored anonymously may differ somewhat for this format. Should researchers need to identify data for retrospective withdrawal, they should ask participants to provide a memorable code or ID number which can be used for these purposes. Care needs to be taken to ensure that such mechanisms are in accordance with current data protection legislation.

We then turn to the issue of withdrawal during an online study. In IMR, a number of points should be noted in relation to ensuring that a participant's right to withdraw is not violated. Two key factors, which make IMR approaches rather different to many offline contexts, should be borne in mind:

a. the typical lack of physical presence between researcher and participants; and

b. the automated collection of data during the research process.

Together, these factors compound the risk that participants might decide to withdraw from a study without this being obvious to the researcher, and after partial (or even complete) data have already been submitted and stored. Online surveys and experiments are prime candidates for this risk. For example, a participant may decide to exit a survey or an online experiment part way through, and do this by closing their internet browser. In such situations it may not be clear whether the participant intended to withdraw their valid consent for the use of any data already stored. To use any such partial data could thus violate a participant's withdrawal rights. Conversely, not using such data where a participant had spent valuable time contributing data that they did intend to be used also raises ethics issues, related to wasting a person's time and not enabling their contribution to be included.

Essentially, in IMR such difficulties need to be anticipated, and withdrawal procedures made clear and as robust as possible. For example, displaying a clearly visible 'exit' or 'withdraw' button on each page of an online survey or experiment is often good practice. Selecting this would ideally lead to a debrief page and perhaps also a statement asking participants if they require their data to be withdrawn, or whether their partial data can be used (this relates also to the principle of scientific value). Also, some situations make it difficult to implement the 'exit' procedures recommended here (e.g. off-the-shelf online survey software solutions may often not incorporate this functionality). A button at the very end of a study confirming consent to use the data or partial data submitted could help here. Arguably, if this has not been verified by a participant, then their data should not be used. Though a caveat is that participants might not notice a final consent button, particularly if it involves scrolling down the screen beyond what is immediately visible. Careful design and presentation are clearly the best way of avoiding any ambiguities,

or mistakes being made, in relation to these issues.

In qualitative approaches, different issues may arise in relation to ensuring participants' withdrawal rights. For example, in an online focus group it is unlikely that a researcher would remain unaware of a participant's wish to withdraw, but extracting the contributions from one individual from the data set may prove challenging (e.g. other group members may refer to them, or their comments, so simply deleting all the text they submitted may not be sufficient). These issues are not specific to IMR, however.

Unobtrusive approaches require particularly careful consideration in relation to withdrawal issues. Although on first impression it might seem that withdrawal issues are not relevant where participants have not given consent in the first place, the possibility and repercussions of individuals finding their contributions (e.g. discussion forum posts, or social media activity) have been used in a research project, and taking issue with this, must be assessed. Indeed, this point also extends to the possibility of others (third parties) finding out that a particular individual's data traces have been used without permission having been gained. The enhanced potential the internet offers for the swift, broad-reach publication of research data and findings, as well as the enhanced access to traces of personal (online) activity for use as potential research data, may increase such possibilities beyond what is normally the case in offline research.

On a legal note, should a person find out that their online posts or traces of activity have been accessed, stored and used as research data, they may have rights under the UK Data Protection Act (2018) to stop these data being processed if they could be linked to them personally. In many cases it is very unlikely that a person will ever find out that their online posts have been used for research purposes. However, this does not preclude the responsibility of the researcher to ensure that maximal anonymisation procedures are implemented. For example, in dissemination activities or depositing data sets, researchers may consider paraphrasing any verbatim quotes so as to reduce the risk of these being traced to source, and participants identified. When paraphrasing, steps must be put into place to ensure that the original meaning of the message is maintained (e.g. relying on inter-rater consensus between multiple researchers).

A further consideration on unobtrusive data collection is that of withdrawing data if the original post is subsequently deleted prior to the research being completed. Once data have been extracted and processed from their original online space, it is unlikely that the researcher will return here. In these cases, as long as the data obtained had met the principles of being deemed to have occurred in 'public' and was handled in accordance with other ethical principles, it is likely that withdrawal procedures will not be needed, unless the data included anything which could be deemed illegal or violating terms of use from its original space. Here again, the principle of proportionality becomes pertinent: considerations of the level of risk/harm must be weighed up against scientific value, the quality and authenticity of reports of research findings, and possible practical issues too.

COPYRIGHT

A further consideration in relation to the use of data deemed to be in the public domain concerns legislative aspects. While personal webpages may appear to be public documents, copyright remains with the author or web hosting company, and indeed many authors ask to be informed if a link is made to the page. In a similar vein, ownership of 'public' content published on social network sites (updates, chat logs, photos/videos, links, reports from activity elsewhere on the web, etc.) often remains with the online service

provider, as does the ownership of the 'private' communications between members that are mediated by the online service. Under these circumstances, it may be prudent to consider whether there are multiple entities from whom permission to use online data should be sought (e.g. individual user) although it is unlikely researchers would need to contact online service providers. While it may in many cases seem impracticable or unnecessary to always gain explicit permission from data owners (e.g. a website company), these legal aspects should be kept in mind, since in some contexts they may be important in protecting both participants and researchers.

PRINCIPLE 2: SCIENTIFIC INTEGRITY

In relation to this principle, the *Code of Human Research Ethics* (2021) notes the importance of ensuring that a research project meets the criteria of 'quality, integrity and contribution'. A noteworthy issue here in IMR is levels of control: In an IMR context the lack of direct physical proximity may impact on levels of control over and knowledge of participant behaviours, characteristics and research procedures. Such lack of control may have an impact on the validity of a piece of research, its findings and conclusions (for example, particularly in experimental designs where tight control over variables is crucial to validity). Related to this point, the *Code of Human Research Ethics* (2021) highlights the potential for harm to arise from the dissemination of inaccurate or misleading information (such as invalid research results and conclusions). An additional relevant consideration pertinent to IMR, particularly relating to big data and data-driven approaches, is the scope for AI/machine learning approaches to generate potentially misleading, inaccurate, or damaging information and inferences, including about individuals and/or research participants (such as predicting likely behaviours, risks or classifying people based on algorithmic models). Questions have been raised (see additional resources) regarding the extent to which such analyses and interpretations derived from applying these techniques can be trusted, and the ethical implications of potentially sharing findings that make use of these techniques.

LEVELS OF CONTROL

The typical greater degree of 'distance' from participants in IMR can lead to difficulties in maintaining levels of control over research procedures and environment. This may be manifested in not being able to control (or verify):

a. who has access to participate;

b. the environmental conditions under which participants are responding (e.g. are they watching television at the same time);

c. participants' feelings, reactions, responses to the research process; and

d. variations in the research procedure due to different hardware and software configurations.

Point a is especially relevant to issues of social responsibility and scientific integrity discussed subsequently. Issues b and d are most relevant to issues of scientific integrity and are also discussed here. Point c relates closely to issues of harm and are discussed further below in relation to maximising benefit and minimising harm.

Regarding variations (between participants) in the participation context and procedural aspects of a study, the key issue is that a lack of control may result in variations occurring that might lead to invalid data and conclusions. This concern is especially pertinent in research designs where tight control over such variations is essential. For example, in a perception experiment it may be crucial to tightly control stimulus presentation parameters (luminosity,

hue, size, etc.); in a memory experiment it may be essential to prevent participants from going back using their browser 'back' button and viewing previous pages. Repeat submissions may also seriously undermine the validity of a piece of research. Data forensics can help in detecting multiple submissions from the same participant (by checking IP addresses, browser and operating system information, pattern of responses, etc). Many commercial online survey platforms incorporate such checks and attempt to prevent multiple submissions as a matter of course. The levels of control required, and those able to be achieved, must be considered for any specific study design when deciding whether an IMR approach can be utilised. Maximising levels of control is possible (e.g. there are various tools available for implementing IMR studies which adhere to standards which can, for example, control presentation formats between different browsers). Control in terms of knowing who has participated – such as being able to verify crucial demographic information – is also relevant to data validity (e.g. in studies looking at gender differences), but can be hard to verify in practice.

A further risk to scientific integrity especially in online questionnaires is the likelihood of 'bots' or other AIs completing paid surveys and therefore being false respondents. There are techniques which may mitigate against this, including using some open-ended questions, captcha, and using skip logic; all of which can help to sift out automated respondents (see additional resources for more information on this).

In general, high levels of control over the details of procedural variables (e.g. calibration of presentation parameters such as screen brightness, font size, etc.) will typically be less important for qualitative approaches such as online interviews, and these may thus be less susceptible to the issues raised above. However, it should also be borne in mind that these contexts can often involve more sensitive topics, and thus the need for control in verifying identity must be carefully assessed. Unobtrusive approaches (e.g. analysing server web logs, and other online sources non-reactively) are less likely than obtrusive approaches to be subject to concerns over lack of control, except perhaps for control over security of any data gathered, so as to protect the personal identity of those who contributed to it. However, the issue of data fairness, validity and integrity arises once more here, particularly in relation to emerging data-driven AI approaches, as mentioned above. Researchers have a responsibility to carefully assess the extent to which any inferences and interpretations that they arrive at, and disseminate, are likely to be valid and correct, and to carefully consider in this respect the use of algorithms and machine learning/AI approaches, given some of the controversies these approaches have generated regarding the interpretations they may lead to and the potential impact on individuals and/or groups. This point relates to the principle of scientific integrity, as discussed here, but also social responsibility, discussed next.

PRINCIPLE 3: SOCIAL RESPONSIBILITY

The *Code of Human Research Ethics* (2021) raises several key points in relation to the issue of social responsibility, including maintaining respect for and avoidance of disrupting social structures, and carefully considering consequences and outcomes of a piece of research. In relation to the first point, IMR which proposes to make use of existing online social groups (e.g. social networking sites, discussion forums, multi-user virtual environments, etc.) must bear this issue in mind.

The issue of public/private domain distinctions online (discussed above, under Principle 1) becomes relevant: intrusions from researchers into spaces considered private by their users may be invasive, unwelcome and socially

irresponsible. This may lead to challenges in studying certain communities whereby members may respond in varied ways from being observed. Where the scientific value of such research is considered very high, this may lead to a researcher needing to make decisions about whether joining a group without disclosure as a researcher (i.e. undisclosed observation) might be most appropriate, in order to avoid disruption and potential harm (e.g. to group levels of trust and cohesion). Decisions on this may be determined by the nature of the data collection. That is, unobtrusively collecting public data is less likely to require disclosure than encouraging individuals within a given community to take part in an online survey or interview. Thus, this issue interacts with that of valid consent, and the individual research context will need to be considered to decide what is most appropriate.

The enhanced scope for (often automatic) widespread dissemination of and access to data generated in IMR must be considered. For example, a researcher may make use of a 'research blog' as a forum for field notes (e.g. as might be done in an ethnographic study); this could very quickly lead to widespread dissemination of information about the study, the data collected and, potentially, the participants taking part. Likewise, researcher participation in an open discussion forum has similar dissemination potential (discussion forum archives are often readily available for anyone to search by topic and view). Indeed, even a researcher highlighting that a discussion forum in a quiet corner of the internet exists somewhere may be unwelcome to its users. Such issues have relevance to considerations of harm, as discussed elsewhere in this document (particularly under Principle 4 below). It is not necessarily the interventions themselves that are potentially harmful, but their possible scope for compromising the anonymity/confidentiality of participants. Researchers should consider such potential unintended consequences.

A further issue relevant to social responsibility is compensation for participants in reactive research (e.g. online surveys). It is common to recruit participants via survey panels or crowdsourced labour marketplaces. In some instances, these offer very low rates of payment. Therefore, researchers should take steps to ensure that participants are not exploited but at the same time, that payment is not disproportionately large so as to potentially promote coercion.

Researchers should also consider how online data collection methods systematically exclude people who have difficulty accessing or navigating the Internet and how this might marginalise the voices of groups who might be already underrepresented in research. For example, an inequality in using the internet is present within society on social, geographical or geo-political grounds. By exclusively collecting data online we may therefore continue to promote inequality and benefit those who are already privileged. Researchers may wish to consider additional data collection methods to canvas the perspectives of these groups, if appropriate.

Finally, it was noted earlier that researchers/RECs need to carefully assess the ethics issues involved in using emerging AI/machine learning techniques, such as those that aim to develop or apply algorithms that can supposedly infer additional information 'baked into data' (such as individuals' likely personal characteristics, existing medical conditions, predicted risky behaviours, and so on). In addition to considerations of scientific integrity/accuracy that become salient when using such techniques, considerations of social responsibility also emerge. Thus, disseminating algorithmically inferred information about individuals, or groups, may be damaging and harmful (perhaps even more so when the inferences may be of questionable validity and/or the groups are already socially stigmatised). The additional resources offered enable interested readers to explore these issues further.

PRINCIPLE 4: MAXIMISING BENEFITS AND MINIMISING HARM

FOR PARTICIPANTS

This principle embodies many of the key points and issues already raised, including ensuring scientific value (maximising benefits) and taking steps to protect participants from any adverse effects arising from the research. Such steps may include gaining valid consent, ensuring anonymity and confidentiality (to minimise harm) and maintaining appropriate levels of control over the research process (to help maximise benefits and minimise harm). As already noted, a lack of control can lead to issues in verifying identity (e.g. determining whether a participant is the minimum age required to give informed consent or detecting multiple submissions). It seems reasonable to propose – so as to not be overly restrictive – that in relation to issues of verifying identity (e.g. restricting participation), a researcher should carefully weigh up any potential harmful effects should a person below the required age (for example) endeavour to and succeed in taking part. Again, the key principle of making ethics checks and procedures proportional to the assessed risks and potential for harm emerges. In high risk situations, researchers should consider whether their research is actually suited to IMR. For example, where research deals with sensitive or adult themes and the age of the participant cannot easily be verified online, researchers should consider whether their research is better suited to being done offline. In low risk situations it may often be sufficient to take a range of steps which can help minimise the likelihood of successful participation by excluded individuals, such as taking participants who enter age details within a certain range to an exit page from which they are unable to re-enter (even if they attempt to return and re-enter with different age information), and only placing participation adverts in spaces where excluded individuals are unlikely to view them.

A lack of control may also prevent the researcher from monitoring participants' reactions and behaviours. For example, this may jeopardise the ability to detect when a participant has withdrawn, and thus properly present debrief information. In relation to this point, deception (by the researcher) raises potential for harm in particular, and in an IMR context the lack of physical proximity with research participants can mean extra care is needed if deception is being proposed. Difficulty in monitoring and responding to participants' (potentially negative) reactions to research procedures, compared with proximal in-person contexts, also creates scope for harm. This means that if doing research involving sensitive topics or where risk is high, alternative mechanisms for minimising risk to participants may need to be considered. Such IMR contexts where levels of control (over who participates, and knowledge of their reactions) are at their lowest would be, for example, an online survey. Procedures such as online real-time interviews, on the other hand, would perhaps offer the greatest levels of control in IMR. The dimension of levels of control must thus be considered in the context of the specific research methods and context.

Threats to anonymity/confidentiality (see earlier comment regarding the relationship between the two) are also relevant to this principle. In some cases it is not always apparent how traceable online data can be, and the nature of risks related to possible re-identifiability of published data sets or outputs (as well as the scope for revealing additional potentially sensitive information) may not be obvious. As noted above, researchers should be aware that in IMR it can be relatively easy to trace quotes which have been published from source material (e.g. as often used in conversation or discourse analysis) to individuals' original postings, using search engines, and that this may compromise their anonymity and hence confidentiality. Serious consideration should be given to whether publishing such traceable quotes requires specific valid consent from the individual, and it should be avoided in any cases where possible consequential risk

and harm to participants is non-trivial. Where it is not possible to obtain informed consent, it is good practice to either omit quotes and just discuss themes in the data, or paraphrase the quotes. As previously mentioned, when paraphrasing it is essential that the original meaning of the message is maintained. It is also important to ensure the researchers remove any unique terms or hashtags that may have been included in the original message; for example, if a user includes a hashtag or term that very few others have used - it can be very easy to identify the original source even if the rest of the message has been paraphrased.

Similarly, publishing the name or address of the website or discussion forum from which data were gathered may compromise the anonymity of individuals or have a negative effect on an online community. Where there is such a risk, it may be argued that this identifying information should not be published alongside any analysis of communication sourced from that site. In some cases it may be clear that the risk of potential harm is low (e.g. large, ubiquitous social media sites; quantitative aggregate data analysis). Additionally, some groups, such as political activists, may welcome the publishing and dissemination of their discussions (though this does not necessarily mean that there are no risks for group members in doing so). In less clear-cut situations, researchers considering naming the location from which their source material was drawn should discuss it with moderators or other gatekeepers of those online services, and take their insights into consideration. The pseudonyms used by posters to web services (blogs, chat rooms, social media, etc.) should be treated with the same respect as a researcher would treat a participant's real name.

The lack of researcher control over confidentiality of participants' identifiable data (despite taking all possible precautions) was mentioned above under Principle 1. For example, law enforcement agencies may subpoena research data. Terms and conditions of any third party applications or software used to assist in data collection should be carefully considered, as well as any third party's compliance with local data protection laws (e.g. procedures which involve storing information/data on servers in different political jurisdictions may often be seen as problematic, and may be prohibited by RECs, especially where personal data are involved). Emailing research participants can also be problematic. When recruiting participants by email, researchers need to be aware that the security of unencrypted email is low, and email content can be inadvertently disclosed on the Internet, local and other computers. Therefore, even the common practice of emailing research participants can, in principle, be problematic. Researchers therefore risk breaching participant confidentiality if they use non-secure e-mail in research or practice, and participants themselves may often be unaware of these risks.

A further breach of confidentiality may derive from using data transcription software which uses a third party to generate automatic written transcription of audio data. Even services which use AI for this purpose are best avoided to stay fully compliant to participant confidentiality policies. Finally, any real-time interviews which take place online such as through video chat should be conducted on secure platforms (e.g. password-protected meeting rooms), software should have sound privacy policies (i.e. not send on data to third parties) and researchers should be connected to the Internet via secure network rather than ones which are freely available in public spaces.

There are potential threats to anonymity in some IMR contexts; for example, where mechanisms for paying participants may use information which makes participants personally identifiable, such as an email address. Even for IMR questionnaires where data are anonymous in the sense of not containing names, addresses or other direct identity information, researchers should be aware that there may be residual risks that participants can nevertheless be identified.

As with questionnaires administered in offline studies, combinations of demographic variables, and/or roles and characteristics, may permit identification (e.g. area, income, occupation, age). RECs may sometimes request a complete listing of the data that are to be gathered from each participant, such as a set of survey questions or an interview schedule (e.g. with particularly sensitive research) so as to be able to make an informed judgement about such risks. In some contexts, though not all, it may arguably be appropriate and necessary for a researcher to provide this. Researchers should also remain aware, as already explained, that despite research data sets appearing to contain no personally identifying information, it is possible that personal identities may be revealed by comparing data sets with other linked sources which do contain such information. Also, additional sensitive information about individuals may be inferred from data sets. This may be achieved, for example, by interrogating traces, such as website browsing history or social media site usage, to statistically predict (e.g. using machine learning algorithms) sensitive personal characteristics (e.g sexual orientation, or political views) that have not otherwise been disclosed by individuals. Whilst in many cases the risk of leaking personally sensitive data in this way may be very low, given more recent developments involving increased attention to big data, machine learning and AI approaches in IMR, researchers should be mindful of these possibilities and take steps to properly identify, assess and reduce any such risks. This will involve properly anonymising research data sets, and carefully considering dissemination and data sharing practices, particularly those that may potentially lead to data (re)identification. There is an increasing need for researchers to publicly share their research data – including depositing data sets in repositories for future use by other researchers – so the ways in which these data sets may be processed, and any associated potential risks as just discussed, requires careful analysis.

FOR RESEARCHERS

As well as there being specific considerations for minimising harm to participants, the same also applies to researchers. There may be instances in which researchers are exposed to sensitive or distressing content, particularly when undertaking research unobtrusively online but also in interview-based research. This is becoming a key discussion point in IMR, with academic papers highlighting considerations about emotional labour, and disclosure of serious risk of harm (see additional resources for more detail on this). Of course these risks may exist in other forms of research but these are perhaps elevated in IMR from the fact there is greater ease in accessing distressing content online and this may potentially be larger in quantity. Additional risks may derive from researchers making use of online communities (e.g. discussion boards, social networking sites) to advertise or disseminate research insights. Indeed, this may draw out unsolicited attention or messages which may be emotionally distressing. There is also the issue that researchers on these platforms may receive unsolicited messages of those seeking urgent help or advice (e.g. people experiencing domestic violence) which may bring on additional pressures to researchers doing IMR.

Another important consideration is researcher, and/or their linked institution, reputation: the ubiquity of, and enhanced scope for dissemination and visibility of findings in, IMR can make researchers/institutions increasingly vulnerable to scrutiny, potentially leading to derogatory attacks that might damage reputations. This risk emerges from the broader dissemination, accessibility and visibility of research activity that online spaces and dissemination practices facilitate (this is not unique to IMR, perhaps, but certainly a prevalent concern). Researchers should therefore consider risks to researchers as well as participants as part of risk

assessment protocols in doing this form of research. A further consideration relates to use of appropriate websites and services. For example, accessing websites for research purposes which relate to illegal activities (e.g. terrorism) may alert authorities and result in legal ramifications. Therefore, researchers should avoid risking their own integrity by accessing websites which are designed around illegal services, goods or activities, without having prior authorisation to do so by the relevant authorities.

Conclusion

In closing, the following points bear repetition. First, the typical principles of ethical research with human participants apply to IMR, and the basics of ethical practice are not changed. However, the implications of these principles for practice may differ in IMR contexts, and aspects of online environments may make particular issues salient in ways they have not been in traditional research. Certain ethics principles may be more or less salient in different types of research design, and the procedures researchers put in place should be proportional to the likely risk to participants and researchers. When planning IMR one should take into account both the existing methodological literature and the fundamental principles of research ethics.

ADDITIONAL RESOURCES

British Psychological Society (2021). *Code of human research ethics*. Retrieved 21 May 2021 from www.bps.org.uk/sites/www.bps.org.uk/files/Policy/Policy%20-%20Files/BPS%20Code%20of%20Human%20Research%20Ethics.pdf

British Psychological Society (2018). *Code of ethics and conduct*. Retrieved 12 November 2020 from www.bps.org.uk/sites/www.bps.org.uk/files/Policy/Policy%20-%20Files/BPS%20Code%20of%20Ethics%20and%20Conduct%20%28Updated%20July%202018%29.pdf

Franzke, A.S., Bechmann, A., Zimmer, M., Ess, C. & the Association of Internet Researchers (2020). *Internet research: Ethical guidelines 3.0*. Retrieved from https://aoir.org/reports/ethics3.pdf

Edelman, N. (2020). *Internet-mediated research in the wake of Covid-19: Dealing with disclosure of serious risk of harm*. Retrieved 10 November 2020 from https://f1000research.com/articles/9-426

Hanna, E. (2019). The emotional labour of researching sensitive topics online: considerations and implications. *Qualitative Research, 19*(5), 524–539. doi:10.1177/1468794118781735

Reynolds, E. (2020). Psychologists are mining social media posts for mental health research – But many users have concerns. *BPS Research Digest*. Retrieved 10 November 2020 from https://digest.bps.org.uk/2020/06/29/psychologists-are-mining-social-media-posts-for-mental-health-research-but-many-users-have-concerns

Rodd, J. (2019). *How to maintain data quality when you can't see your participants*. Retrieved 10 November 2020 from www.psychologicalscience.org/observer/how-to-maintain-data-quality-when-you-cant-see-your-participants#.XHlMd1Z1Szs.twitter

Simone, M. (2019). *Bots started sabotaging my online research – I fought back*. Retrieved 10 November 2020 from www.statnews.com/2019/11/21/bots-started-sabotaging-my-online-research-i-fought-back

UK Research Integrity Office (2016). *Good practice in research: Internet-mediated research*. Retrieved 17 November 2020 from https://ukrio.org/new-guidance-from-ukrio-internet-mediated-research

the british
psychological society
promoting excellence in psychology

St Andrews House
48 Princess Road East
Leicester LE1 7DR, UK

☎ 0116 254 9568 www.bps.org.uk info@bps.org.uk

Incorporated by Royal Charter Registered Charity No 229642 | REP155/06.2021