Wishart, M. & Kostanski, M. (2009). First Do No Harm: Valuing and Respecting the ‘Person’ in Psychological Research Online. *Counselling, Psychotherapy, and Health,* 5(1), The Use of Technology in Mental Health Special Issue, 300-328.

Counselling, Psychotherapy, and Health
www.cphjournal.com
cphJournal.com

First Do No Harm: Valuing and Respecting the 'Person' in Psychological Research Online

Madeline Wishart
Victoria University

Marion Kostanski
Victoria University

Contact:
Madeline Wishart
madeline@madelinewishart.com.au

Abstract

The advent of the Internet has heralded broad changes in organisational and personal communication, commerce and information sharing. These technological advances have resulted in a shift in the methodologies and environments in which psychological research is undertaken. Transcending geographical barriers, the Internet offers a quick, convenient and inexpensive method of data collection from a large population of widely dispersed participants within a non-normative population. The Internet can be utilised effectively to eliminate or reduce the power differential between the researcher and the participant, providing a forum in which to communicate in a transparent and reflective dialogue. The portable functionality and accessibility of the laptop computer, combined with advances in wireless technology provide the researcher with remarkable flexibility and mobility. Research can be conducted anywhere and at any time. At face value, the Internet and its many applications (e.g. email, Internet Relay Chat, social networking websites, multi-user environments, newsgroups, bulletin boards, electronic mailing lists, instant messaging, web pages) could be perceived as the panacea and substitute for the heavily sampled population of undergraduate psychology students, yet as an instrument of research methodology, it is not without its weaknesses and challenges. As such, it is imperative that researchers consider the ethical, moral, technical and legal implications to adequately protect participants, whilst promoting innovative and methodologically sound research. This chapter examines the issues and considerations involved in undertaking a psychological study online. The difficulties associated with obtaining informed consent, privacy and confidentiality, deceptive techniques, debriefing, beneficence and the personal investment attributed to pseudonyms are addressed. Current ethical guidelines for conducting research via the Internet are reviewed and recommendations for best practice are presented.

Introduction

The Internet wields the potential to reshape the face of psychological research, transforming the means by which research is conducted; data collected, collated and analysed; and research published (Kraut et al., 2004; Nosek, Banaji, & Greenwald, 2002; Wishart & Kostanski, 2004). With a forecasted 2 billion global users online by the year 2011 (Computer Industry Almanac, 2006), the Internet is a crucible for the human experience, offering an electronic forum to voice our feelings, desires, interests and opinions (Eysenbach & Till, 2001). As such, the inimitable breadth of applications online (i.e. e-mail, Internet Relay Chat (IRC), multi-user environments, newsgroups, social networking websites, bulletin boards, electronic mailing lists, instant messaging (IM), web pages) offers researchers a rich latent source of social, behavioural and archival data (Kraut et al., 2004; Mann & Stewart, 2000; Robinson, 2001). The social interaction idiosyncratically inherent in these varied applications provides researchers with a unique opportunity to gain insight into a myriad of psychological constructs and phenomena in nonclinical settings (Wishart & Kostanski, 2004) and into the discourse and phenomena peculiar to this electronic medium (Kraut et al., 2004; Sharf, 1999).

The benefits that the Internet affords researchers must be counterbalanced with careful consideration of whether the researcher can conduct their study morally and ethically within this infrastructure (Porr & Ployhart, 2004). Whilst Kraut et al. (2004) contend that, fundamentally, online research is no more problematic nor of greater risk to participants than conventional research methods, this methodology is still in its infancy. Researchers must not only be conversant in their chosen field but also have a sound understanding of the Internet, its varied applications and the technology underpinning them (Frankel & Siang, 1999; NIMH, 2003). However, the dynamic nature of the Internet makes it increasingly difficult for researchers without an educational background in computer science to keep abreast of technological advances and comprehend the ethical issues that entail (Keller & Lee, 2003; Mann & Stewart, 2000; Sharf, 1999).

There has been considerable debate around the ethical implications of conducting research online, and this debate has traversed the schools of academia exploring Internet research scholarship (Clark, 2004; Krantz & Dalal, 2000). It has been widely agreed that traditional ethical guidelines and standards are challenged by the alterations in spatial, temporal, verbal and sensory aspects of human interaction online (Azar, 2000; Kralik, Warren, Price, Koch, & Pignone, 2005; Kraut et al., 2004; Suler, 2000). Whilst many of the issues remain unanswered, it is important that researchers seriously consider the ethical implications of their research online or they risk not only harming the participants in their study but the very phenomena under investigation (Berry, 2004; Hamilton, 1999). Many researchers have lobbied for universal ethical guidelines for online research, contending that at present, there are few boundaries to guide researchers in utilising the World Wide Web (DeLorme, Zinkhan, & French, 2001; King, 1996).

The establishment of a universal set of ethical guidelines for any research undertaken online could see researchers abrogating the extant ethical codes that govern research practices. It would be more appropriate to follow what Ess and Jones (2004) referred to as “ethical dogmatism” and a strict adherence to the codes that guide traditional research methods. The institutional review boards (IRB) and professional principles that guide us in our practice in the real world must be applied to our pursuits into online research (Azar, 2000). For psychologists, these are the Australian Psychological Society’s (APS) Code of Ethics (2002) or the American Psychological Association’s (APA) Ethical Principles of Psychologists and Code of Conduct (2002). In fact, the APA Code of Conduct (2002) specifically states “if this Ethics Code establishes a higher standard of conduct than is required by law, psychologists must meet the higher ethical standard (p. 2).”

Informed Consent

Autonomy or respect for persons is one of the three fundamental tenets identified in the Belmont Report (1978) that forms the foundation of the current ethical and legal frameworks for the protection of participants in human subjects research. It ensures that individuals are treated with autonomy, dignity and respect (Flicker, Haans, & Skinner, 2004; Frankel & Siang, 1999). In practice, the principle of autonomy is ordained through the process of informed consent. This integral process involves providing prospective participants with clear, concise and accurate information about the research; empowering them with the necessary knowledge to make an informed decision as to whether or not they choose to participate in the study (Wishart & Kostanski, 2004).

Frankel and Siang (1999) delineated three key facets in the informed consent process:

1. Presenting information about the research to participants.
2. Ensuring comprehension.
3. Attaining and securing a voluntary commitment to participate.

They contend that in online research it is the latter two facets that are problematic.

Presenting Information about the Research to Participants

It is relatively easy to present plain language statements and consent forms in an online format. Both documents can be simply and effectively incorporated into the research web site and viewed online, or downloaded and printed by participants as hard copies (Frankel & Siang, 1999; Wishart & Kostanski, 2004). The challenge is in obtaining the handwritten signature from participants that legally signifies their consent to participate in the study (Frankel & Siang, 1999). Technologically, this hurdle could be overcome by the use of digital signatures to authenticate one's consent. However, the cost and accessibility of this software remains largely prohibitive to the average domestic Internet user (Porr & Ployhart, 2004; Stern, 2004).

Ensuring Comprehension

Advocates of Internet research argue that the presence of a legally binding signature does not automatically ensure comprehension, even in offline studies. The perceived power differential and the degree of trust between the participant and the researcher can result in participants consenting to participate in studies they do not truly understand (Kersting, 2004; Wishart & Kostanski, 2004). In this sense, the very nature of Internet research has the potential to diminish the effects associated with the inevitable reactivity in research with human participants. The physical absence of the researcher, anonymity and perceived level of privacy, combined with the higher degree of automation inherent in online studies significantly reduces experimenter bias, demand and social desirability characteristics (Bordens & Abbott, 1999; Siah, 2005). This has considerable positive implications for the reliability and validity of Internet studies.

Conversely, participants may be more distrustful of the legitimacy of online research, as they cannot plainly see the researcher or other participants (Siah, 2005). This could result in difficulties obtaining a statistically significant sample size and impact on the honesty and breadth of participants’ responses.

In conventional research methodologies, the researcher is typically present to address and respond to any questions participants may have about the research, before signing the consent form (Varnhagen et al., 2005). Mann and Stewart (2000) contend that in Internet research, the effectiveness of the question period can be impeded by several key factors:

a. Time constraints.

b. The online synchronicity of both the researcher and the participant.

c. The reluctance of the participant to engage with the researcher due to the perception of formality which may be attributed to textual dialogue.

d. The inability of the researcher to gauge any non-verbal cues the participant may display, indicating that they do not truly comprehend the nature and the purpose of the study.

However, a study by Varnhagen et al. (2005) suggests that the effectiveness of this question period could also be queried in studies using more traditional methodologies. The study compared traditional pen and paper informed consent to online informed consent, and overall found no significant differences between traditional methods and online methods of informed consent. Indeed, in the experimental group that used traditional paper informed consent, not one participant asked the researcher a question prior to signing the consent form. In both groups (online and standard paper format), the participants read the documents quickly and subsequently recalled very little of the information in the consent form (Varnhagen et al., 2005).

Attaining and Securing a Voluntary Commitment to Participate

Logistically, it is no more difficult attaining and securing a voluntary commitment to participate in online studies than it is in their offline counterparts. Click to accept buttons, downloadable documents, online registration prior to commencement, e-mail and old fashioned snail mail can all be employed to facilitate the consent process (refer to Table 1). The key word in this facet of the informed consent process is the term *voluntary*. In fact, it could be argued that it is central to the entire principle of autonomy, and poses one of the fundamental concerns in the debate over the ethics of online research – *is it necessary to obtain informed consent in Internet studies?*

Hudson and Bruckman (2004) raised the following questions in relation to informed consent:

1. “Is it ethical to enter a chatroom and record the conversation for research purposes?
2. Is it sufficient to announce the researcher’s presence and offer users a way to opt out of participation?
3. Is it feasible to announce the researcher’s presence but only record data if participants type a command to opt in?” (p. 128).

The answer is unequivocally no. International Review Boards (IRB) reviewing conventional research methods would not accept these means of obtaining informed consent; therefore they should not be acceptable in online research methodology. The principle of beneficence compels researchers to minimise any potential harms (i.e. emotional or psychological distress, social disadvantage, loss of privacy and public exposure). If the process of obtaining consent is likely to harm an online community in any way, the researcher should design a web site, electronic mailing list, IM or chat room specifically for the purposes of the research (Hudson & Bruckman, 2004).

Table 1

Informed Consent: Ethical Concerns and Recommendations

Ethical concerns	Recommendations
1. Recruiting participants	a). Obtain written permission from moderators of sites before posting advertisements for research studies on their web sites or electronic mailing lists (Michalak & Szabo, 1998).
2. Informing participants about the research study	a). A plain language statement should be visibly presented on the research web page. It should be written clearly using simple language.
3. Physically obtaining informed consent	a). Design a “click to accept” button (Kersting, 2004). b). Request digital signatures (Kraut et al., 2004; NIMH, 2003) c). Incorporate an informed consent statement in a portable document format (PDF) into the research web site that can be downloaded by participants, signed and returned to the researcher by post (Kraut et al., 2004; NIMH, 2003). d). Post an informed consent statement to participants with a pre-paid postage return envelope (NIMH, 2003). e). Create a password protected web site, requiring participants to register online prior to their participation (Nosek et al., 2002).
4. Ensuring comprehension of informed consent	a). Pre-test the plain language statement and informed consent statements (Kraut et al., 2004). b). Anticipate participants questions about the research and present a list of “Frequently Asked Questions” on the research web page (NIMH, 2003). c). Design a “click to accept” button for each point in the informed consent statement (Kraut et al., 2004). d). Ensure that participants cannot access the survey or discussion group until they have checked all of the boxes in the online informed consent statement (Porr & Ployhart, 2004). e). Require participants check a box indicating that they have understood the informed consent statement and what is involved in participating in the research and have no further questions about the study (Porr & Ployhart, 2004) f). Develop a questionnaire or quiz to assess participants understanding of the plain language statement (Kraut et al., 2004; NIMH, 2003).

	g). Communicate with participants via e-mail, telephone, IM, or in a chat room purposively established for the study, to respond to any questions they may have about the research (Flicker et al., 2004; NIMH, 2003; Suler, 2000).

D*eceptive Research Techniques*

As in conventional research there may be phenomena or populations that researchers contend necessitate the use of deceptive techniques. The Australian National Statement on Ethical Conduct in Research Involving Humans (NHMRC, 1999) – the governing body for research in Australia - and the American Psychological Association's Code of Conduct (2002) explicitly state that deceptive techniques are in direct conflict to the principle of autonomy, as consent is not of a *voluntary* nor *completely informed nature*. However, if the data cannot feasibly be obtained via any other means, other than by deception, concealment or covert observation, the NHMRC stipulates that the researcher must ensure that:

d. "participants are not exposed to an increased risk of harm as a result of the deception, concealment or covert observation;

e. adequate and prompt disclosure is made and debriefing provided to each participant as soon as practicable after the participant's participation is completed;

f. participants will be able to withdraw data obtained from them during the research without their knowledge or consent;

g. such activities will not corrupt the relationship between researchers and research in general with the community at large" (NHMRC, 1999, p. 51).

Adhering to these four clauses is challenging, if not impossible in Internet studies involving the use of deception. Is not deception by its very nature harmful? Whilst, this is not a debate about the merits of deceptive research methods, online research employing deceptive measures most certainly may result in psychological or emotional distress, discomfort or loss of privacy and public exposure. Finn and Lavitt’s (1994) infamous study of computer-based self-help groups for sexual abuse survivors provided an early example of this, when they cited the specific group names, dates and times of postings; quoting unwilling and unsuspecting participants verbatim in their publication. With this much identifying information anyone could access the BBS network (cited by name) and look up previous postings to discover the true online identities of the participants.

Employing deceptive measures to obtain data from online communities is tantamount to lurking, and is not viewed favourably by netizens. This in itself poses a significant risk, as members do not like to feel as if they have been observed and studied (Eysenbach & Till, 2001). Whilst the ethical concerns regarding the adequate debriefing of participants can be overcome when setting up purpose built online experiments (refer to Table 2), these strategies are difficult to enact when studying qualitative phenomena in existing online communities. Without prior arrangement through the informed consent process (refer to Table 2), it is very difficult to ensure that participants can be promptly and adequately debriefed at the completion of data collection. Online participants can suddenly become inactive if they answer a phone, go to the bathroom, become disinterested or succumb to any number of distractions that would impede their participation. With the click of a mouse, participants can voluntarily withdraw themselves from the study, or their participation may be involuntarily terminated due to program error, a computer or server crash or a power failure (Nosek et al., 2002). Can the researcher ensure that they are able to contact participants to provide adequate debriefing and attain their permission to use the data obtained from them during the research?

Table 2

Debriefing: Ethical Concerns and Recommendations

Ethical concerns	Recommendations
1. Presentation of debriefing material	a). Incorporate a debriefing statement in a PDF file into the research web site that can be downloaded by participants (Kraut et al., 2004; NIMH, 2003). b). Augment the debriefing statement with additional material on the research web site e.g. further information, referral lists, crisis telephone numbers, researcher’s contact details (Kraut et al., 2004; NIMH, 2003). c). Anticipate participant’s concerns about the research and present a list of “Frequently Asked Questions” on the research web page. This solves the dual purpose of indicating that these concerns are normal and to be expected (NIMH, 2003; Nosek et al., 2002). d). Design a “click to accept” button for each separate point in the debriefing statement (Kraut et al., 2004). e). Build a “withdraw from the study” button into each web page, which automatically directs participants to the debriefing page, even if they choose to leave the study early (Nosek et al., 2002).
2. Ensuring adequate debriefing	a). Pre-test the debriefing statement (Kraut et al., 2004). b). Require participants check a box indicating that they have understood the debriefing statement and have no further questions about the study (Porr & Ployhart, 2004). c). Develop a self-report questionnaire or quiz to evaluate participants’ reactions (Kraut et al., 2004; NIMH,

	2003). d). A debriefing page could be designed to pop up automatically if participants prematurely close the browser window (Nosek et al., 2002). e). Create a “contact the researcher” button on each web page that automatically opens an untitled e-mail in a new window addressed to the researcher. f). Communicate with participants via e-mail, telephone, IM or in a chat room purposively established for the study, to respond to any concerns or questions they may have about the research (Flicker et al., 2004; NIMH, 2003; Suler, 2000).
3. Providing debriefing in the event of technological difficulties, e.g. computer or sever crash, broken Internet connection, program error or power outage	a). Require research participants to supply an e-mail address prior to participation in the study and e-mail debriefing statements at a later date (Nosek et al., 2002). b). Supply participants with an e-mail address, to which they can send questions or comments about the study (Nosek et al., 2002). c). Determine and discuss emergency protocol with participants in the event of an involuntary connection (Kraut et al., 2004; NIMH, 2003). d). If debriefing via e-mail, specify in the plain language statement the number of follow-up e-mails that will be sent to participants in the event of technical difficulties and/or at the completion of the study.

Privacy and Confidentiality

The greatest risk to those participating in online research is not derived from the experience of participating in the research itself, but of potential breaches in confidentiality, where personal or identifiable information is accessed, intercepted or circulated involuntarily (Kraut et al., 2004; Wishart & Kostanski, 2004). This can occur at any stage during the research process, from data collection and storage, to the dissemination and publication of results (Frankel & Siang, 1999; Wishart & Kostanski, 2004). Breaches or compromises to the data generally occur via two avenues: ethical or moral, and technological concerns. The former is largely subjective and dependent upon the researcher’s understanding of online culture and ethical sensitivity; whilst the latter is reliant upon the researcher’s technological knowledge, skills and resources (Pittenger, 2003).

Perceived Level of Privacy

There has been considerable debate across academic disciplines as to whether the Internet is essentially a “public” or a “private” domain (Eysenbach & Till, 2001; Robinson, 2001; Stern, 2004). Researchers have posed endless questions attempting to conclusively resolve this debate (Eysenbach & Till, 2001; Kraut et al., 2004; Robinson, 2001; Suler, 2000). Is the site only accessible via a password, registration or subscription (Eysenbach & Till, 2001; Robinson, 2001; Suler, 2000)? Does the person or group associate a certain level of privacy with the site (Eysenbach & Till, 2001; Kraut et al., 2004; Robinson, 2001; Suler, 2000)? What number of netizens regularly use the application (Eysenbach & Till, 2001)?

The traditional dichotomy between “public” and “private” becomes blurred in relation to the Internet, and the perception of privacy appears to be largely subjective (Pittenger, 2003; Wishart & Kostanski, 2004). The Internet promotes a false sense of security in online users, as they are generally interacting with the various applications it offers from the comfort and privacy of their home or workplace (King, 1996; Kraut et al., 2004). Many people are unaware that they inadvertently leave identifying information –

like footprints – through cookies, e-mail addresses or IPs whenever they visit a web site (Kraut et al., 2004). Walther (2002) argued that as textual discourse on the Internet is publicly accessible, it does not actually constitute human subjects research. As such, he contends that researchers are not bound by the restraints of IRBs human subjects regulations. However, other authors believe terms like publicly-private, privately-public (Berry, 2004), semi-published and semi-private (Hudson & Bruckman, 2004) are more appropriate, suggesting a less rigid adherence to existing spatial categories.

The fire fuelling this debate is principally derived from the desire of researchers to access the rich latent source of social, behavioural and archival data available on the Internet (Wishart & Kostanski, 2004). If the various applications on the Internet are deemed to be public in nature, then researchers do not need to obtain the consent of online authors to use their written word as data (Frankel & Siang, 1999; King, 1996; Kraut et al., 2004). With the lack of face-to-face interaction in online studies (particularly in asynchronous forms of text-based communication), it is easy for researchers to fall into the trap of objectifying the text on their computer screen, failing to show respect for the very real individuals behind the keystrokes (King, 1996; Stern, 2004).

Intellectual Property

If one adheres strictly to the doctrines of autonomy, justice and beneficence, than the debate over public versus private domain and human subjects research is largely negated. The Australian National Statement on Ethical Conduct in Research Involving

Humans (NHMRC, 1999) unequivocally states that research activities must not jeopardise the relationship between researchers and the general community. Clark (2004, p. 252) most eloquently articulated this position stating “it makes sense in terms of sustaining the goodwill of my participants for me to treat all data that I collect about and from the group as strictly private unless given permission to see it otherwise”. Furthermore, there is a fervent online culture of individuals who use the Internet explicitly to express their voice. As such, the publication of direct quotations could be considered tantamount to intellectual property theft (Eysenbach & Till, 2001; Lawson, 2004).

Screen Names: Privacy and Personal Investment

Users, netizens and cybercitizens typically expend considerable time and energy developing their screen name, pseudonym, handle, nick (nickname), moniker or avatar; and therefore place a significant personal investment in them. This is an important consideration in the minimisation of potential harms to participants (Frankel & Siang, 1999; King, 1996). Individuals often unwittingly use identifying information in the creation of their screen name, such as portions of their actual offline name or initials; physical characteristics; the names of their street, suburb or post code; the names of pets or family members; age or year of birth; and favourite hobbies, sports, activities or food (e.g. Jane Doe 1989, Ivanhoe blonde 28, Rex St Kilda 91). Most places of employment incorporate staff members’ real names in the creation of their email addresses and usernames for computer-mediated business activities. Many people naively use these email addresses to register for and engage in online applications, with little forethought to the highly identifiable content they are leaving behind. In fact, in numerous asynchronous applications registrants’ full email addresses are displayed to other group members (Lawson, 2004). Given this, it appears imprudent for researchers to unconditionally guarantee confidentiality to participants. Whilst every effort should be given to maintain the privacy and confidentiality of participants, they should be forewarned that the very nature of the medium makes it very difficulty to unequivocally implement and police it (Clark, 2004; Lawson, 2004).

Technological Concerns

The infrastructure of the Internet and the hardware that it operates from has evolved exponentially since its commercialisation two decades ago (Keller & Lee, 2003). To remain relevant, technology must continue to evolve at this rapid pace. This continual state of flux is challenging to the average researcher in psychology, who must become au fait not only with their own field of interest, but with the technology they wish to embrace methodologically to conduct their research (Frankel & Siang, 1999; Keller & Lee, 2003). There are many considerations, risks, moral and ethical dilemmas that may arise throughout the research process, which the technological novice is likely to be unaware of upon embarking on an Internet-mediated study. Mental health professionals typically do not possess the technological training to adequately prepare them for a comprehensive understanding of the serious moral and ethical breaches to participants’ privacy and confidentiality that can occur in this dynamic and complex medium (Mathy, Kerr, & Haydin, 2003). As Mathy et al. (2003, p. 84) succinctly stated "…the mere ability to send and receive e-mail and navigate the World Wide Web is a grossly insufficient basis on which to decide to provide clinical services or conduct clinical research online". Researchers should realistically assess their own technological knowledge and skills, developing an understanding of their limitations, prior to initiating online research. Gaps should be addressed via consultation and collaboration with experienced professionals in information technology, software development, ethics and Internet-mediated research (Fisher & Fried, 2003; Mathy et al., 2003; National Institute of Mental Health, 2001).

Table 3

Privacy and Confidentiality: Ethical Concerns and Recommendations

Ethical concerns	Recommendations
1. Ensuring the anonymity of research participants	a). Inform participants that whilst every effort will be made to ensure their anonymity, it cannot be guaranteed (Porr & Ployhart, 2004). b). Explicitly list the steps taken to maintain anonymity (Flicker et al., 2004). c). Consult with experts to limit the access of search engines to any forums purposively established for the research, particularly IRC, IM and bulletin boards (Eysenbach & Till, 2001; Flicker et al., 2004). d). If participants are invested in their pseudonym, suggest they develop an alternate pseudonym for the study. e). Disguise all pseudonyms and online communities (Cherny, 1999). f). Refrain from using any details that identify a particular online forum or community (Cherny, 1999). g). Any individuals that could be identified online or in real life by their published descriptions in research, could be divided into multiple characters, as opposed to being

		described as a "whole" (Cherny, 1999).
2.	Protecting the privacy and confidentiality of participants	a). Inform participants that confidentiality cannot be assured (Clark, 2004). b). Explicitly list the steps taken to preserve confidentiality and inform participants of the sources of all potential breaches in confidentiality (APS, 2004; Flicker et al., 2004). c). Inform participants of how the data will be used, recorded, stored and disseminated (Fisher & Fried, 2003; NIMH, 2003). d). Only collect demographic data that is pertinent to the research (Michalak & Szabo, 1998). e). Privacy screens could be utilised in the office to shield monitors when viewing particularly sensitive data (Fisher & Fried, 2003).
3.	Protecting the confidentiality of the communication channel between the researcher and participants	a). Inform participants of all sources of potential breaches in confidentiality (APS, 2004; NIMH, 2003). b). Employ encryption software in data transmission, storage and recovery (Kraut et al., 2004). c). Inform participants that e-mail is not a secure form of communication and may be intercepted by a third party, or read by another individual sharing the hardware at either end of the communication (Fisher & Fried, 2003). d). Remind participants to be aware of their physical surroundings when participating in online research in public places, i.e. university, library, open plan office (NIMH, 2003). e). Recommend that participants avoid writing any confidential information in e-mail or IM unless encryption software is used (Fisher & Fried, 2003). f). If an electronic mailing list is used in the data collection process, remind participants to reply directly to the researcher and not to the group as a whole (Michalak & Szabo, 1998). g). Consult with technology personnel to ensure virus and security protection software is up to date (Fisher & Fried, 2003).
4.	Maintaining confidentiality during data storage	a). Consult or seek training in the technology of securing information over the Internet (National Institute of Mental Health, 2001). b). Consult with technology personnel on the storage of

			data on your institutional or personal hard drive, server or via any removable and rewritable data storage devices (Fisher & Fried, 2003).
		c).	Password protection and encryption should be employed for all sensitive data, directories and files (APS, 2004; Fisher & Fried, 2003).
		d).	Avoid sharing passwords and change them regularly, steering clear of the obvious and easily deduced (Fisher & Fried, 2003; Reips, 2002).
		e).	Only provide access to the directories containing the research data to those directly involved in the research process (Kraut et al., 2004).
		f).	If research assistants are required to access the research data, ensure that they are trained appropriately, to adequately protect the confidentiality of participants (Fisher & Fried, 2003).
		g).	Do not store any identifying information directly on the research web site (NIMH, 2003).
		h).	Ask participants not to use their surnames or formerly established pseudonyms as their log-in for the study (NIMH, 2003).
		i).	Securely store any portable (i.e. laptop computer) and removable data storage devices (i.e. floppy disks, optical disk storage, USB flash memory drive) (Fisher & Fried, 2003).
		j).	Distort any auditory or visual images of participants (Fisher & Fried, 2003).
		k).	Collect and record any demographic data separately from the research data, using an arbitrary code to link the two (Kraut et al., 2004).
		l).	Remove any specific references to the type of online domain (e.g. IRC, bulletin boards, e-mail, IM) from the data, and store this information separately (King, 1996).
		m).	Consult with an expert when disposing of, or upgrading a computer to guarantee all traces of the data stored are permanently removed (Fisher & Fried, 2003).
5.	Using quotations in research publications	a).	Offer participants the option to negotiate the level of their consent with regards to the use of their pseudonym, text and authorship of their discourse in a published academic paper (Lawson, 2004). Lawson (2004) identified five levels of consent that participants could select from:

	1. no publication of pseudonym or text. 2. publication of *either* the pseudonym *or* the content with strictly no identifying information. 3. publication of *either* the pseudonym *or* the content with strictly no identifying information on the proviso they may review the paper prior to publication. 4. publication of both the pseudonym and the content, crediting the participant as the author of their discourse. 5. publication of both the pseudonym and the content, crediting the participant as the author of their discourse, on the proviso they may review the paper prior to publication (p. 93).

Conclusion

A tenuous balance currently exists between the advantages of Internet-mediated research and the ethical risks inherent in this medium (Mathy et al., 2003). Whilst the medium in which the research is conducted and the methodologies may have changed, the code of ethics governing human subjects research has not. The fundamental ethical tenets of beneficence, autonomy and justice still regulate our research practices (Ess & Jones, 2004; Kralik et al., 2005). These principles must be adhered to and researchers need to act with moral responsibility and integrity in Internet-mediated research, just as they would if encountering participants in a face-to-face setting (Azar, 2000).

The principle of beneficence dictates that researchers are required to minimise potential risks and possible harms to participants (The Belmont Report, 1978). The greatest threat in online research is to the autonomy, privacy and confidentiality of participants (Kraut et al., 2004; Wishart & Kostanski, 2004). The loss of reputation and trust in the research community at large is also a significant concern when zealous researchers undertake studies online without the appropriate training, collaboration or consultation. If researchers do not possess the technological expertise to ensure that all potential harms are minimised to the fullest extent of their power, than more traditional methodologies should be adhered to (Mathy et al., 2003).

If mental health professionals continue to flood the World Wide Web at the rate with which they have over the past decade, then perhaps IRBs should consider mandating a core subject in online research methodologies for undergraduate and postgraduate students. Ideally, the National Health and Medical Research Council (NHMRC) could develop a set of ethical guidelines that work within the existing ethical framework to govern our research practice online, reducing the moral and ethical ambiguities that are rife with this dynamic and extraordinary medium.

The recommendations suggested here are by no means comprehensive or definitive. However, they do offer some rudimentary guidelines for researchers considering online experimentation. A constructive multidisciplinary discourse should be fostered between academics and professionals from the mental and medical health sciences, technology and ethics to promote innovative, methodologically sound, ethically and morally driven research online.

References

American Psychological Association. (2002). Ethical Principles of Psychologists and Code of Conduct. *American Psychologist, 57*(12), 1060-1074.

APS. (2004). Guidelines for providing psychological services and products on the Internet.   Retrieved 1st April, 2004, from http://www.psychology.org.au/members/ethics/6.4_1.asp

Azar, B. (2000). Online experiments: Ethically fair or foul? *Monitor on Psychology, 31*(4).

Berry, D. M. (2004). Internet research: Privacy, ethics and alienation: An open source approach. *Internet Research, 14*(4), 323-332.

Bordens, K. S., & Abbott, B. B. (1999). *Research design and methods: A process approach* (4th ed.). Mountain View, California: Mayfield Pub. Co.

Cherny, L. (1999). *Conversation and community: Chat in a virtual world*. Stanford, Calif.: CSLI Publications.

Clark, D. (2004). What if you meet face to face? A case study in virtual/material research ethics. In E. A. Buchanan (Ed.), *Readings in virtual research ethics: Issues and controversies* (pp. 246-261). Hershey, PA :: Information Science Publishing.

Computer Industry Almanac. (2006, 4 January). Worldwide Internet users.   Retrieved 16 March, 2006, from http://www.c-i-a.com/pr0106.htm

DeLorme, D. E., Zinkhan, G. M., & French, W. (2001). Ethics and the Internet: Issues Associated with Qualitative Research. *Journal of Business Ethics, 33*(4), 271.

Ess, C., & Jones, S. (2004). Ethical decision-making and Internet research: Recommendations from the AoIR Ethics Working Committee. In E. A. Buchanan (Ed.), *Readings in virtual research ethics: Issues and controversies* (pp. 27-44). Hershey, PA :: Information Science Publishing.

Eysenbach, G., & Till, J. E. (2001). Ethical issues in qualitative research on Internet communities. *British Medical Journal, 323*(7321), 1103.

Finn, J., & Lavitt, M. (1994). Computer-based self-help groups for sexual abuse survivors. *Social Work with Groups, 17*(1-2), 21-46.

Fisher, C. B., & Fried, A. L. (2003). Internet-mediated psychological services and the American Psychological Association ethics code. *Psychotherapy: Theory, Research, Practice, Training, 40*(1-2), 103-111.

Flicker, S., Haans, D., & Skinner, H. (2004). Ethical dilemmas in research on Internet communities. *Qualitative Health Research, 14*(1), 124-134.

Frankel, M. S., & Siang, S. (1999, 20 June 2003). Ethical and legal aspects of human subjects research on the Internet. June 10-11. Retrieved 16th June, 2003, from http://www.aaas.org/spp/dspp/sfrl/projects/intres/main.htm

Hamilton, J. C. (1999). The ethics of conducting social-science research on the Internet. *The Chronicle Of Higher Education, 46,* B6-7.

Hudson, J. M., & Bruckman, A. (2004). "Go away": Participant objections to being studied and the ethics of chatroom research. *Information Society, 20*(2), 127-139.

Keller, H. E., & Lee, S. (2003). Ethical issues surrounding human participants research using the Internet. *Ethics & Behavior, 13*(3 (Print)), 211-219.

Kersting, K. (2004). When done right, Internet research yields rewards. *Monitor on Psychology, 35*(2), 52.

King, S. A. (1996). Researching Internet communities: Proposed ethical guidelines for the reporting of results. *The Information Society, 12,* 119-127.

Kralik, D., Warren, J., Price, K., Koch, T., & Pignone, G. (2005). The ethics of research using electronic mail discussion groups. *JAN Journal of Advanced Nursing, 52*(5), 537-545.

Krantz, J. H., & Dalal, R. (2000). Validity of web-based research. In M. H. Birnbaum (Ed.), *Psychological experiments on the Internet* (pp. 35-60). London: Academic Press.

Kraut, R., Olson, J., Banaji, M., Bruckman, A., Cohen, J., & Couper, M. (2004). Psychological research online: Report of Board of Scientific Affairs' Advisory Group on the conduct of research on the Internet. *American Psychologist, 59*(2), 105-117.

Lawson, D. (2004). Blurring the boundaries: Ethical considerations for online research using synchronous CMC forums. In E. A. Buchanan (Ed.), *Readings in virtual research ethics: Issues and controversies* (pp. 80-100). Hershey, PA: Information Science Publishing.

Mann, C., & Stewart, F. (2000). *Internet communication and qualitative research: A handbook for researching online*. London: Sage.

Mathy, R. M., Kerr, D. L., & Haydin, B. M. (2003). Methodological rigor and ethical considerations in Internet-mediated research. *Psychotherapy: Theory, Research, Practice, Training, 40*(1/2), 77-85.

Michalak, E. E., & Szabo, A. (1998). Guidelines for Internet research: An update. *European Psychologist, 3*(1), 70-75.

National Institute of Mental Health. (2001, April 26, 2001). Internet-based Research Interventions: Risk minimisation strategies.   Retrieved 26 November, 2003, from http://www.nimh.nih.gov/research/cyber.cfm

NHMRC. (1999). *National statement on ethical conduct in research involving humans*. Canberra, Australia: National Health and Medical Research Council (NHMRC).

NIMH. (2003). Internet-based Research Interventions: Issues and suggestions chart. Retrieved 23 March, 2006, from http://www.nimh.nih.gov/researchfunding/interventionschartjuly03.pdf

Nosek, B. A., Banaji, M. R., & Greenwald, A. G. (2002). E-research: Ethics, security, design, and control in psychological research on the Internet. *Journal of Social Issues, 58*(1), 161-176.

Pittenger, D. J. (2003). Internet Research: An Opportunity to Revisit Classic Ethical Problems in Behavioral Research. *Ethics & Behavior, 13*(1), 45-60.

Porr, W. B., & Ployhart, R. E. (2004). Organisational research over the Internet: Ethical challenges and opportunities. In E. A. Buchanan (Ed.), *Readings in virtual research ethics: Issues and controversies* (pp. 130-154). Hershey, PA :: Information Science Publishing.

Reips, U.-D. (2002). Standards for Internet-based experimenting. *Experimental psychology, 49*(4), 243-256.

Robinson, K. M. (2001). Unsolicited narratives from the Internet: A rich source of qualitative data. *Qualitative Health Research, 11*(5), 706-714.

Sharf, B. F. (1999). Beyond netiquette: The ethics of doing naturalistic discourse research on the Internet. In S. Jones (Ed.), *Doing Internet research: Critical issues and methods for examining the Net* (pp. 243-257). Thousand Oaks, Calif.: Sage Publications.

Siah, C. Y. (2005). All that glitters is not gold: Examining the perils and obstacles in collecting data on the Internet. *International Negotiation, 10*(1), 115-130.

Stern, S. R. (2004). Studying adolescents online: A consideration of ethical issues. In E. A. Buchanan (Ed.), *Readings in virtual research ethics: Issues and controversies* (pp. 275-287). Hershey, PA :: Information Science Publishing.

Suler, J. (2000). Ethics in cyberspace research: Consent, privacy and contribution. Retrieved July 18, 2003, from http://www.rider.edu/~suler/psycyber/ethics.html

The National Commission for the Protection of Human Subjects of Biomedical and Behavioural Research, & United States Department of Health Education and Welfare. (1978). *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research* (No. DHEW Publication No. OS 78-0012). Washington DC: United States: Government Printing Office.

Varnhagen, C. K., Gushta, M., Daniels, J., Peters, T. C., Parmar, N., Law, D., et al. (2005). How Informed Is Online Informed Consent? *Ethics & Behavior, 15*(1), 37-48.

Walther, J. B. (2002). Research ethics in Internet-enabled research: Human subjects issues and methodological myopia. *Ethics And Information Technology, 4*, 205-216.

Wishart, M. E., & Kostanski, M. (2004). *The ethical implications of conducting psychological research on the Internet.* Paper presented at the 39th Annual Australian Psychological Society Conference, Sydney, Australia.