STAKEHOLDER SAFETY IN INFORMATION SYSTEMS RESEARCH

Dr. R.H. Barbour
School of Computing and Information Technology
Unitec
Carrington Road
Mount Albert
New Zealand
Email: bbarbour@unitec.ac.nz

ABSTRACT

Information Communication Technology (ICT) researchers adapt and use tools from reference and cognate disciplines. This application of existing tools outside the context of their development has implications beyond the immediate problem context. ICT researchers have access to a wide variety of data sources including newer ones, such as the Internet, that may bring unexpected outcomes. ICT research can impact on researchers, their institutions and the researched in unexpected ways. People so affected are the stakeholders in ICT research activities. Reputations, welfare and property may be put at risk by unplanned events described in this paper. Legal aspects of ICT research are broadly identified and linked to the tort of negligence. The Social Research Association's Code for researcher safety is described and its application extended to include the Internet as a potential data source. A common set of underlying ethical principles is identified suggesting that the ICT researcher can refine particular research protocols for specific social contexts.

Keywords: stakeholder, researcher safety, research protocol, ethics, Internet, social research, Information Communication Technology, negligence, information privacy, information access, information ownership, intellectual property.

INTRODUCTION

It is now twenty years since the publication of two papers, one by Moor (1985) and another by Mason (1986). For Moor computer ethics in 1985 was characterised among other things by a policy vacuum in how computers should be used. For Mason there were four issues: information privacy, information access, information as property and information accuracy. Bynum's (1999) paper is true to its title and provides a succinct summary of the history of ethics in computing. Bynum attributes the term *computer ethics* to Maner who used the term in the late 1970s. Floridi and Sanders (2002) suggest that there are at least five positions in the literature as to how computer ethics should be viewed. Johnson's (2004) paper in (Floridi, 2004) advanced a view that computing introduced a new species of generic moral problems. The underlying ethical problems remain to appear in a new computer related domain. Other thinkers including Maner (1980) believe that computing introduces radically new ethical issues that will eventually supplant conventional ethical issues as the newer issues come to predominate. This paper makes no case for any particular view but returns to each of Mason's four issues and addresses them within the perspective of stakeholder safety and in relation to modern societies that are becoming increasingly litigious. The particular motivation in this paper is to encourage the people using social research methods to develop protocols to protect the welfare of all stakeholders involved in the research process.

The focus of Information Communication Technology (ICT) research is extending from interest in hardware and software to close interest in the human aspects of ICT. Researchers are more frequently carrying out in-depth research into human perceptions of, and responses to, ICT uses and contexts. Research interactions, discussed more fully below, involve risks to the human subjects of the research and the researchers who carry out the research. This work, often qualitative and using social science methods, exposes researchers to the hazards of mistaken intention, misinterpretation of instructions and behaviour, and claims of unacceptable actions that, if they arose, could be interpreted in law as negligence (Cecil, 1991). Specific examples where researchers may be at direct physical risk are: conducting interviews in remote or high-risk locations; delivering and collecting questionnaires from homes and flats in high-risk areas; and conducting interviews in social clubs or, in some situations, conducting focus group research in, and into, other cultures. Protocols, describing actions to reduce the consequences of such hazards, take many forms and learning about them is part of the training of most professions. The goal of such training is to ensure that the researcher carries out the research in a way that ensures that the research activities do not result in damage or harm to either the public or the researcher.

It is easy to understand why the medical professions have very clear protocols for medical people in their dealings with patients. It is not so clear why ICT researchers should meet analogous requirements when dealing with respondents, particularly when the interactions occur in the World Wide Web through the medium of the Internet. An indication of the recent emergence of concern for social science researcher safety is expressed in the form of Guidelines for personal safety during work (Kirklees Community Council, 2005) adapted from the Social Research Association (SRA, 2004). In (Leonard, 2001) the gender specific responses to the hazards of field study in Anthropology are reported as being passed down by word of mouth. The recent adoption of social science research methods in ICT has resulted in a vacuum in tacit practice that might otherwise protect individual researchers. Following Moor's (1985, and Moor and Bynum's, 2002) concern over a vacuum in how computers should be used, this paper attempts to address an analogous issue of the vacuum related to how (ICT) researchers and their institutions should act to keep stakeholders safe. In the first major section, the purposeful application of social science research methods in ICT contexts is discussed. Possible difficulties arising from potential failures in practice are discussed in the first sub-section. Suggestions are outlined that could address research safety in the second and third sub-sections. I describe, in the second major section, a generic view of the law related to negligence and involuntary exposure to hazard. In the third major section, stakeholders are identified and strategies for resolving ICT related research problems are discussed. In the fourth major section, the Social Research Association (SRA) Code is described and some details discussed. In the last section, the Internet-World Wide Web or cyberspace is considered as a data source and some special aspects of cyberspace research further considered.

PURPOSEFUL RESEARCH USING SOCIAL SCIENCE REFERENCE DISCIPLINE METHODS

It is well understood, at the disciplinary level, that social science researchers see people and the data related to them as being worthy of a special duty of care. With respect to persons, subjects of research expect that they will retain the four rights of ownership of their own information (Mason, 1986). Those ownership rights include the ability to access information stored about them and to correct information that is incorrect. Rights to personal information extend to privacy, that is the right to block access to information, and lastly, the right to have ownership and management of information regarded as intellectual property (Moor, 1985). In essence, this position places people and their data as ‘ends’ in themselves, not means to the ‘end’ of research. At a pragmatic level, this view is held because continued goodwill in the form of public cooperation is essential for continued social ICT research.

The overarching purpose of social research is to better understand people and so implicitly, in some way, improve their welfare by reporting the outcome of the research. The metric for that enhanced welfare is the balance of the person’s perceptions of the good and bad consequences of the research as experienced. The actions of social researchers come under scrutiny if it can be shown that the experience of the people participating in research does not meet the expectations of the relevant discipline or profession. Such expectations are described in codes of ethics and in the guidelines provided by institutional research committees for researchers seeking ethical approval for their research (Johnson, 2004).

In the context of research proposals encompassing research using human subjects, the deliberations of people serving on ethics committees serve three purposes. The first is to ensure that the respondents are not harmed by the research activity. The second is to ensure that either the activities or the outcomes of the research do not harm the good name of a discipline, reflecting the good name of the institution. The third, more recent, is to ensure that the welfare of researchers pursuing legitimate research (an academic activity) as paid employees, is not put at unacceptable risk. This third element in the trio of ethical responsibilities is a recent addition (Johnson, 2004) to the concerns of academic employers who in turn have passed the responsibility on to academics themselves. The current disciplinary academic solution to the problem of reducing risk is to require research be supported by proposals that must be approved by an ethics committee responsible for ensuring that the proposed research will not result in a litigatable outcome. In this process, experienced academics who have already shown that they understand what is required to ensure that research risks are identified and their effects mitigated, help colleagues to plan and carry out appropriate research actions. Such knowledge and experience is accumulated incrementally in disciplines as they grow and develop. ICT academics, often coming from disciplines other than social science, have not had the length of development time required to ensure that, as academic supervisors, they have sufficient experience of newer social research methods to offer wise council to younger colleagues. Lack of consultation with colleagues in the social sciences exacerbates a potentially avoidable situation. Failure to provide appropriate advice on the consequences of proposed research exposes academic institutions to the possibility of claims of negligence discussed in the next section.

Negligence

As suggested, there is a wealth of experience in other disciplines describing research risks, identifying hazardous situations and proposing mitigating strategies. It is to this body of work that I turn to identify, in analogous contexts, those possibly unforeseen events sketched in the opening paragraphs that may affect the ICT researcher. It is assumed that research is being carried out in a way that does not intentionally harm subjects. It is also assumed that the research has more than nuisance value. I begin by examining the worst possible outcome, that of a claim of negligence. In the research context, negligence is taken to mean failing to adhere to current discipline or employer protocols for the conduct of research. In law that might be seen as is reported by Cecil (p 38, 1991) as: "getting wrong that which another practitioner more often than not would get right" Successful claims of negligence have been shown to reflect five failures related to duty, reasonableness, causation, damage and remoteness. I describe them in the following section adapted from Cecil (1991), and dealing with an English view of negligence in architecture. Cook & Gilbert (2004) deal with a New Zealand point of view across a number of disciplines.

The five situations leading to possible negligence claims are:

Duty (Risks, the Law and Negligence)

The Law on negligence varies in detail from profession to profession and from country to country. Most western jurisdictions require of citizens a duty of care in actions to protect other members of the community from unreasonable risk of harm.
It is usually accepted that:

- Parents have a duty to care for their children.
- Landlords have a duty to tenants to keep a residence habitable.
- Professionally, engineers have a duty to ensure the bridges they build do not collapse.

Each duty is applicable to a particular responsibility in a context. Professional activities require a higher standard of care than the average person in society. In the discussion that follows it is noted that case law is extremely limited as to research related academic negligence. Jackson and Powell (2002) a widely referenced series on Professional Negligence do not provide a separate chapter on either teaching or academic negligence.

Reasonableness

Problems arise when claims are made that a person has failed in their duty. The test is: Would a reasonable person in a similar situation have done the same thing? It is usual to apply the criteria with respect to reasonableness in two ways. The first is to take a hypothetical person and ask what would they have done. The second is to ask whether the actions taken by the actual person were reasonable under the circumstances at the time. Failure on either test is examined either in an ethics hearing or in a Law Court

Causation

Claims about research outcomes could be scrutinised on the basis of showing the damage was caused directly by negligently carrying out the research activities. Research outcomes could also come under scrutiny because of a more distant consequential claim where it can be shown that the risks of harm were foreseeable.

Damage

Damage can take many forms: physical, financial, psychological or social. Remedies under Law are complex and fall outside the scope of this discussion but are intended to offer compensation for the actions taken that caused harm.

Remoteness

Actions that cause damage must be part of normal expectations of the course of events. It must be reasonable, again, to have expected the damage under the circumstances.

Defences

A ‘defence’ may remove claims under the Law that harm was caused by negligence. In essence, in a research context, a defence would be advanced to show that the research outcomes were a result of actions outside the claims. Defences may arise if it can be shown that the person making a claim took actions that contributed to the harm. A defence may arise if it can be shown that the person was informed of the nature of the research and had signed a consent form that identified the possibility of harm. Lastly, a defence can take the form of a counter-claim that the harm was caused by the person’s actions in the context. The items listed above are well worth avoiding and share sufficient common ground to justify practises being developed that guide and protect researchers from the most obvious problems. Policy statements in university research guidelines should identify the causes of negligence listed in general above and attempt to protect staff by insisting on approved and signed informed consent being sought from subjects. Not only do researchers wish to avoid harm to other people but also to themselves, an issue examined in the next section.

Solutions to the Problem of Researcher safety

The first area to look for information that will reduce harm to researchers is in the ethical guidelines of disciplines and organisations. Ethics committees, charged with administering those guidelines provide three types of support in the form of:

- accumulated professional and lay experience for researchers.
- aggregate classes of problems for presentation to a group of individuals who have a shared memory about the conduct of research.
- standard contexts for classes of research related-problems that do not easily lend themselves to administrative solution, such as check-list based evaluations.

The second area to look for guidance is the codes of ethics in the professions. Both ethics committees and codes of ethics have the primary focus of ensuring participant safety. As mentioned above, almost never, until recently, is there a stated concern with researcher safety (SRA, 2004) or the safety of other people considered below in Figure One. However, in the mid to late 1990s, concerns over work place safety (CFHS, 2005) of people who dealt directly with the public (Bentley, 2005) led the Social Research Association to consider developing a Code of Practice for social researchers that recognised the particular risks associated with carrying out social research. SRA (2004) and CFHS list the following items as matters of concern:

- Risk of physical threat or abuse.

- Risk of psychological trauma or consequences as a result of actual or threatened violence or the nature of what is disclosed during the interaction.
- Risk of being in a compromising situation in which there might be accusations of improper behaviour.
- Increased exposure to general risks of everyday life and social interaction: travel, infectious illness, accident.

The CFHS (2005) lists the following item as a matter of concern:

- Risk of damage to, or theft of, equipment and data

Dealing with these threats is the responsibility of both the employer and the researcher. In most countries, an employer must meet work place safety requirements of protection from harm (Kirklees Community Council, 2005). An employee is expected to adhere to instructions provided during employment to avoid embroiling the employer in legal claims as well as for the simple common sense reason of avoiding harm to oneself. Before looking in more detail at the Code, stakeholders in social research will be identified.

THE STAKEHOLDER VIEW

The extent of the impact of involvement in the consequences of research has been shown (McCosker, Barnard & Gerber, 2001) to be wider than previously thought. They show that data collection in areas of high stress or increased sensitivity may have impacts on all the people involved. McCosker et al.'s (2001) view is that researchers and other people involved in the research task may require support and counselling because of their involvement. People that may be affected include those providing data, entering and coding the data, reporting the research, supervising and reviewing the outcomes of the research process (see Figure One). These newly identified elements have arisen from the context of studies of natural hazards, disasters, familial and other abuse and criminality, newsroom and chat room interactions. It is suggested that taking a stakeholder/participant view of research into sensitive issues will result in better social research and safer, more informed, communities. Particular care is required where ICT research involves children and other vulnerable individuals or groups.

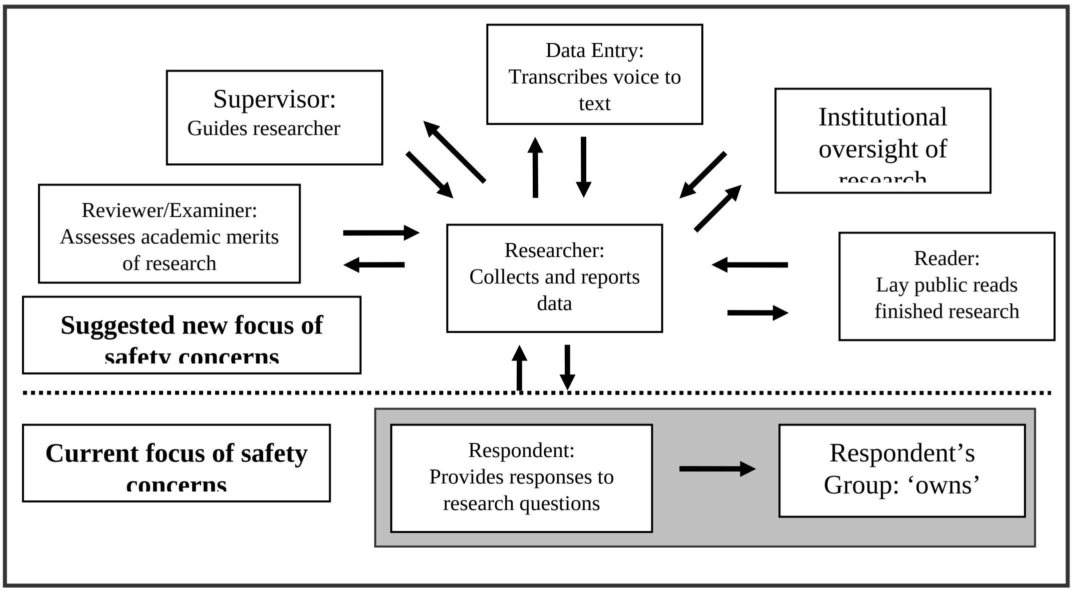
Data Entry:
Transcribes voice to text
Supervisor:
Guides researcher
Institutional oversight of research
Reviewer/Examiner:
Assesses academic merits of research
Researcher:
Collects and reports data
Reader:
Lay public reads finished research
Suggested new focus of safety concerns
Current focus of safety concerns
Respondent:
Provides responses to research questions
Respondent's Group: 'owns'

Figure 1. Participants potentially affected by IT showing current (lower part of the figure) and suggested new foci of concern (including all stakeholders).
(adapted from McCosker, Barnard & Gerber, 2001).

Safety of Person and Property

Concerns for researchers' safety centres on security of person and property are outside those matters traditionally addressed by ethics committees. However, recent changes in law in many countries have gradually altered the nature of the workplace into one where responsibility for workplace safety is shared between employer and employee. Ethics committees might reasonably be expected to request information about research protocols where the research context could place people or property at risk. The most useful contribution would be in the continuing provision of a single point of reference (an institutionally sanctioned but independent ethics committee) to which the acceptability of critical aspects of research protocols for staff and students could be confirmed. The SRA Code formalises the issues related to safety during research.

THE SOCIAL RESEARCH ASSOCIATION CODE (SRA CODE)

The SRA Code (SRA, 2004) describes research responsibilities, budgeting and planning, safe research designs, assessing risks, preliminary preparation for fieldwork, precautions during interviewing, handling risk situations, safety of the public and facilities for debriefing. The Code is thorough, but not exhaustive, in considering aspects of the ICT research protocols where human subjects are concerned. Critical aspects of field research are considered below, then the Internet as a data source is examined from a researcher's point of view.

In the field

A single researcher becomes more exposed to risk during the actual data gathering stages of research where the research takes place in the ordinary milieu of private spaces whether on-line or work or home spaces. Concern for researcher safety may be heightened should the research be about sensitive topics, such as marginal or illegal uses of ICT systems (stealing software, phishing, or hacking systems). Institutions have a role in developing research protocols that protect employees from the worst excesses of other computer users. Universities have a special duty of care to protect student researchers during their research activities (Figure One). Research supervisors have a role in ensuring that risk assessments are carried out and that people selected to collect data have adequate training in following accepted protocols. Where research is carried out in public spaces risk assessments should include concerns over transport to and from data collection locations. Where on-site work requires a lengthy period of stay away from home suitable safe accommodation should be identified. Community leaders and Police should be consulted for advice on local cultural norms and safe data collection locations should the topics or locale be deemed unsafe either generally or at particular times of the day.

Safety concerns begin during the development of research topics and in the formative stages of research proposals. Choices are always open with respect to research questions, data collection methods, data sources, interview sites, paired data collection, timing of data collection. While risk can rarely be removed from data collection, care at the stage of developing research proposals is a prudent strategy that can remove potential risks through careful guidance in topic choice.

Choosing to interview in a public place during hours when many people are in the vicinity is preferable to interviewing in a home late a night. Seeking background information about respondents and their life contexts can provide information that reduces the number of unknown elements during interviews. Lodging schedules for data collection with supervisors and, in high risk areas, to the Police ensures people who might need to be called on know broadly what is planned.

Research designs tied to the relevant reference discipline literature will alert researchers and their supervisors to potential problems resulting from the type of data being sought. Special care should be taken to complete background reading in reference disciplines on the use and misuse of particular tools and techniques. Some topics may invoke strong responses, especially when the respondent feels threatened, that cannot always be predicted. In any case, exit strategies should be considered by supervisors and discussed with researchers so that the consequences of unpredictable outcomes can be avoided. Prior research into maps of the physical surroundings of the interview area as well as a visit with a friend to the site may be required. Suitable exit strategies in more hazardous situations may include escape via known routes, moving to close proximity with a trusted associate, catching a waiting taxi or car.

Early visits to an interview area during the day may help establish styles and modes of dress that will enable blending in with the local cultural norms. Valuable property, and equipment should be kept out of sight. Carrying a cell phone, personal ID, a covering letter on institutional letterhead and a personal alarm are all good practice in many contexts. Cell phones can usefully be programmed with a single button press number recall in an emergency. A cell phone can be used to create a record of an interview if a call is placed to an answer phone. A schedule of planned activities can be lodged with trusted persons. Regular calls to a base can help ensure that research activities are monitored.

Researchers often spend time in the field simply observing the context and, without involvement, becoming familiar with possible subjects. Additional briefing about local cultural norms can avoid behaviour that is provoking, or is inconsistent with gender expectations, gestures or language or expected social distance. Co-supervisors from reference disciplines can provide essential guidance for less experienced researchers by working through plans for field research. While most social research is carried out either face-to-face or by paper, newer electronic media have particular attractions of ease of use and amenability to advanced computer based processing and analysis. The Internet is considered in the next section together with some of the ethical and safety issues that may arise in ICT research.

THE INTERNET

The Internet fulfils an important role in connecting people and information across the globe in a more or less open fashion. What people write or are prepared to say in any medium may not be an accurate reflection of their actual views. The same view holds for Internet accessible media as data sources. Scepticism is a suitable strategy when evaluating Internet sources as a research tool or information derived from the Internet as suitable data for research purposes.

Internet based Research

The communications that make up the Internet include email, chat rooms, discussion boards, on-line auctions, web sites and newsrooms. The major distinction that might occur is that between public and private space in cyberspace. That is whether the person making the communication intends it to be a public pronouncement or believes that the audience is restricted and therefore that the communication is essentially private (Eysenbach & Till, 2001). In the same paper Eysenbach & Till (2001) state: that where matters raised in cyberspace communications have potential to impact on the lives of people, including the researcher, steps must be taken to treat the emerging data as coming from a private space. On the other hand, people's contributions in the public parts of cyberspace can be assumed to have the same status as letters to the editor, that is, just opinions. Clues to private space are the requirement to 'join' the group by registration, or password, or other means of identification. Some apparently open cyberspaces have clear expectations that the space is private and usually inform potential participants by announcement on the home page of the web page.

Public or private cyberspace

The primary issue here is for the potential respondent(s) to determine whether their contributions are public or private. Possible research uses of Internet communications are described by (Eysenbach & Till, 2001) as:

- passive analysis where the researcher simply records the contributions for subsequent study. The researcher is not identified or active in the communication in any way other than observing and recording that interaction.
- active analysis where the researcher participates in the communications in order to confirm the accuracy of contributions.
- public analysis where the researcher declares themselves to the group and gathers information, in the form of semi-structured "interviews", on-line "focus groups", or surveys, from the other participants.

Key issues for researchers in cyberspace are: whether informed consent, privacy, and confidentiality issues require particular actions in the new media of the Internet. If the standard of acceptance of research activities is to allay respondent's concerns, it is clear that all three issues should be taken into consideration when designing cyberspace research. Consent rarely can be waived except where privacy and confidentiality are rigorously protected by carefully anonymising data so that neither the individual nor their group can be identified in the results.

Gaining informed consent, where it seems a personal space is being investigated should be carried out in an open and straightforward manner. The approach may be direct, to an email address or indirectly, to the group as a whole. The list owner may help and would at least understand something of the cultural dynamics of the group members. Eysenbach & Till, (2001) advise caution in accepting Internet contributions as there is no practical way of verifying contributions that are without attribution. Even with attribution and email confirmation it is difficult to distinguish between actual and fabricated contributions. Verbatim quotes can also be problematic as data sources because they may easily be traced back to original contributors. While the anonymising process may have been thorough, simply keying a string of words into a search engine is likely to return the Internet resource and the author from which it was drawn. It is easy to make connections between data and persons that may then led to breaches of privacy, loss of confidentiality and ultimately, misuse of another person's intellectual property (Eysenbach & Till, 2001). The three key points are: to keep distance from the data, distance between the data sources and distance between the people and the way the data is reported. Clearly, the Internet poses new challenges to people deciding how to interact with the rich data sources it offers. Among the issues that Eysenbach & Till (2001) identify are: privacy, vulnerability, potential harm, informed consent and intellectual property.

The issues of: data security, privacy, intellectual property, confidentiality of sources, right to correct data remain on the Internet, as in any other context. The apparent ease of access to data does not remove responsibility from researchers considering possible harm, or from seeking consent to use other people's contributions. Because matching data sets is easy to carry out with publicly available search tools such as Google, particular care is needed to ensure that string matching does not reveal personal details that would otherwise be inaccessible. Researchers plan to publish, make public, the outcomes of their research. Thus a special duty of care is required to ensure that Internet participants' rights to privacy are not trampled over in the process of carrying out research.

Equally, researchers considering using the Internet as a data source should be mindful of the particular risks of providing their personal data during the research process. Any data requested for verifying identity should be that related to the sponsoring university or institution or responsible committee where there is any possibility of negative outcomes. Creating a Hotmail disposable address can further anonymise email communications. Google requests for web sites dealing with Dos and Don'ts on the Internet provide more generic advice and are good discussion starting points when working through research protocols with supervisors and other researchers.

Such is the rapid change in societies in general and the Internet in particular that any one approach is unlikely to find lasting acceptance or applicability. Hence , in the literature examined no one protocol has been identified as being preferable. Rather, current practice has seen the identification of a number of key considerations that should be addressed when protocols for a particular research data collection process is developed for a particular research context. Eysenbach & Till (2001) argue for the development of best practice protocols. The speed of growth and complexity of both global society and the Internet suggests a more agile approach is appropriate. A more contextually specific approach is proposed. This approach is aimed at using the established underlying ethical principles described above, supported by reasoned context specific protocols. Research protocols would ideally be negotiated among stakeholders in full awareness of the special character of newer media, technologies and the actors in ICT social contexts. In the next section, the major points raised in this paper are summarised.

SUMMARY

Social research methods are being increasingly applied to many ICT problem contexts where people and technology are involved. Aspects of this extension, related to legal consequences, should matters prove unsatisfactory, were discussed. Attention has been drawn to wider aspects of professional relationships with the community. The research process was examined by considering a stakeholder view of research activities. The extent of research engagement in the research context has raised issues related to whether participation is active or passive when Internet sourced data is used. The issues relating to public and private cyberspace have been identified as concerns for both researcher and respondent. Social research may harm some potential research subjects because of their particular vulnerabilities so special care is required when, for example, subjects are children. Potential harm may extend to communities, so care is required where minorities are of particular research interest. Informed consent is usually required from human subjects but may, exceptionally, be waived if public data is examined retrospectively in a passive anonymised way that does not cause harm to those stakeholders whose data is being researched. Confidentiality is a crucial element in ensuring privacy for individuals. Modern search engines enable global searches for text that may link text quoted in research to identify an individual person. Where quotes are used from newer data sources, particularly from Internet sources, informed consent to use those quotes is a must.

People own their creations including personal data in any form of media. Attribution is the usual means of recognising written intellectual property. Seeking permission to use those contributions is also a usual requirement. The Internet, as a data source, offers new possibilities for research yet few protocols have been developed to ensure stakeholder safety while the research is conducted. Safer practices for researchers were identified and briefly discussed extending from matters of data security to personal safety to safety of equipment. The practices of social research will continue to be informed by public debate and researcher experience. Universities, professions and research institutions will find proactive responses based on ethical principles more acceptable than reactive responses to the many ethical issues surrounding social science research in ICT. Taking a stakeholder view indicates that there is much work needed in the areas of developing local protocols acceptable to people in particular contexts in particular cultures as well as protocols for international contexts where data is gathered across cultures.

REFERENCES

Bentley, J. (2005). Suzy Lumplugh Trust. Retrieved 27 Nov, 2005, from http://www.suzylamplugh.org/home/history.shtml

Bynum T.W. (1999) A Very Short History of Computer Ethics. APA Newsletters on Philosophyand Computers. Spring Feruary 1999, (Last accessed Wednesday, 10 May 2006) http://www. southernct.edu/organizations/rccs/resources/research/introduction/bynum_shrt_hist.html.

Cecil, R. (1991) Professional Liability. Legal Studies and Services Publishing Ltd. The Bath Press, Bath.

CFHS. (2005, 18 November 2005). Standard Operating Procedures. Retrieved 25 Nov, 2005, from http://www.ichs.qmul.ac.uk/research/sop/safety.html

Cook, P & Gilbert, M., (2004) Professional Liability. New Zealand Law Society Seminar. June 2004.

Kirklees Community Council, K. M. (2005). Research and Consultation Guidelines: Researcher Safety. Retrieved 24 November, 2005 from http://www.digitv.org.uk/How_to_Guide/ Developing_a_DiTV_service/Step_by_Step/Research/researchersafety.asp

Eysenbach, G., & Till, J. E. (2001). Ethical Issues in Qualitative research on Internet Communities. British Medical Journal, 323, 1103-1105.

Floridi, L., & Sanders, J. W. (2002). Mapping the foundationalist debate in computer ethics. Ethics and Information Technology, 4, 1-4.

Floridi, L. E. (2004). Philosophy of Computing and Information: Blackwell Publishing Ltd., Oxford

Jackson, R. M. & Powell, J. S. R., (2002). Jackson and Powell on Professional Negligence (Common Law Library). London: Sweet & Maxwell. ISBN 0421792205

Johnson, D. (2004). Computer Ethics. (In Floridi 2004., pp 65-75)

Leonard, D. (2001). A Woman's Guide to Doctoral Studies. Buckingham: Open University Press, Buckingham

Mason, R. O. (1986). Four Ethical Issues of the Information Age. MIS Quarterly, 10(1), 4-12.

Maner, W (1978, 1980), Starter Kit on Teaching Computer Ethics (Self published in 1978. Republished in 1980 by Helvetia Press in cooperation with the National Information and Resource Center for Teaching Philosophy).

McCosker, H., Barnard, A., & Gerber, R. (2001). Undertaking sensitive Research: Issues and Strategies for Meeting the Safety needs of all participants. Forum: Qualitative Social Research, 2(1).

Moor, J. (1985). What is Computer Ethics? Metaphilosophy, 16(4), 266-275.

Moor, J., & Bynum, T. W. (Eds.). (2002). Cyberphilosophy The Intersection of Computing and Philosophy. Malden, MA: Blackwell Publishing Ltd., Oxford.

SRA. (2004). A Code Of Practice for the Safety of Social Researchers. Retrieved 24 Nov, 2005, from http://www.soc.surrey.ac.uk/sru/SRU29.html